NHIN Workgroup
Transcript
January 7, 2010

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good morning, everybody. If you could please take your seats. Good morning. Welcome to the HIT Policy Committee's NHIN Workgroup Meeting. The topic today is authentication. This is a federal advisory committee. It's being operated in public. There will be minutes posted on the ONC Web site in a week or so, and the public will have an opportunity to comment at the close of the meeting.
Just let me remind workgroup members, there are a number of workgroup members on the telephone this morning. If you'd please remember to identify yourselves, as well as those in the room for proper attribution. With that, we'll go around the table and introduce the committee members, beginning with Todd Park.

Todd Park – HHS – CTO
Hello. I'm Todd Park, the CTO of HHS.

John Blair – Taconic IPA – President & CEO
I'm John Blair. I'm president of Taconic IPA.

Tim Cromwell – VHA – Director of Standards & Interoperability
Tim Cromwell, Director of Standards and Interoperability for the Department of Veterans Affairs.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Wes Rishel with Gartner.

David Lansky – Pacific Business Group on Health – President & CEO
David Lansky, Pacific Business Group on Health.

Arien Malec – RelayHealth – VP, Product Management
Arien Malec from RelayHealth.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Carol Diamond with Markle.

Neil Calman - Institute for Family Health - President & Cofounder
Neil Calman, Institute for Family Health.

Christine Bechtel - National Partnership for Women & Families – VP
Christine Bechtel, National Partnership for Women and Families.

Latanya Sweeney – Laboratory for International Data Privacy – Director
Latanya Sweeny, Carnegie Melon University and Harvard University.

Jim Borland – SSA – Special Advisor for Health IT, Office of the Commissioner
Jim Borland, Social Security Administration.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
Micky Tripathi, Massachusetts eHealth Collaborative.

Doug Fridsma – Arizona State – Assoc. Prof. Dept. Biomedical Informatics
Doug Fridsma, ONC.

Harley Geiger – Center for Democracy & Technology – Staff Counsel
Harley Geiger with the Center for Democracy & Technology.

Judy Sparrow – Office of the National Coordinator – Executive Director
And I believe we have a number of workgroup members on the telephone. Marc Probst, are you there?

Marc Probst – Intermountain Healthcare – CIO
Yes, I am.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anybody else on the phone lines, please? Okay. With that, I'll turn it over to Dr. Lansky.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you, Judy. Good morning, everyone. First, let me thank you all for making time to join us on this early, early part of the year. It feels like it's July already two or three days into the year, so we have a very busy and aggressive agenda to tackle the issues around authentication today. I want to really thank the staff for having worked so diligently, including over the holidays, to make it possible for this meeting to come together on pretty short notice and preparation time.

As we'll see in a few minutes, the staff has done some great work in framing the issues and in recruiting our witnesses today to help us be better informed about these issues, so I think we're in a good position. Of course, I especially want to thank those of you who have come today to share your expertise with us and having taken the trouble to prepare written testimony and then come here to this meeting. We really appreciate it, and I know it'll be very valuable to help us get our work done.

The agenda for today, as you've all seen, I imagine, is a few introductory comments by myself and Danny Weitzner, who I hope will be here shortly, and then Dave Riley, who hopefully will join us in a few moments. He's in today's bad traffic. Will talk us through some of the context for the authentication discussion, and then we have three panels, including a group of federal experts describing the activities of the federal government, and then a number of you from the private sector to help us understand what's happening there.

We'll then have some time for public comment, any of you who wish to give us your thoughts at 12:30. We'll do that. We'll have a lunch break. We'll then continue the meeting at 1:30 with a discussion among the committee members regarding what we think we're understanding from the testimony that we've heard. Then the meeting will adjourn at 2:30. With that, let me set up at least a couple of thoughts from my point of view and then Doug, I think, will walk us through some of the ONC background on this issue.

How we come to this point and what we're after here, we are a branch of a policy committee on the standards committee, and so our interest is in understanding what can the federal government and its various partners do to facilitate the rapid adoption of meaningful use by eligible providers and hospitals? We want to better understand what are the key infrastructure elements needed to facilitate health information exchange in support of meaningful use. In other words, we're not interested in, or at least I'm not, in a deep dive into the technical issues around authentication or the various technical options that are before us. We really want to understand the policy ramifications of the approaches that are available in the marketplace and where can we be helpful to stimulate the growth in that marketplace and the adoption of health information exchange in a secure, reliable, robust fashion.

I think it's a challenge for all of us to keep our discussion at a level that many of us on the committee who are not highly technical can understand, and be best informed to make policy recommendations to ONC and others who are interested in this area. So I hope you'll help us understand this in context. To do that today, Doug, I think, will set us up with some of the background information, so why don't we go ahead and do that, Doug?

Doug Fridsma – Arizona State – Assoc. Prof. Dept. Biomedical Informatics
Thank you very much. I just want to welcome everyone and thank you for everybody participating and all of the good feedback that we've received. I think the first thing is that I want to make sure that we frame our discussion and continue to make sure that we're moving in a direction that will be helpful to support meaningful use and the exchange of healthcare information.

Our initial charge to this group was to create a set of recommendations for a policy and technical framework that would allow the Internet to be used for the secure, standards based exchange of health information in a way that is both open to all and that fosters innovation. This, I think, is the second of the meetings that we've had that is trying to understand and get feedback about the policy and the technical framework that will allow that to occur. The reason for this is that much of the work in meaningful use and the criteria that has recently been made publicly available this past week requires the exchange of health information among providers and with patients.

And in taking a look at those things, it's clear that one of our foundations to this exchange of information is the ability of a doctor or a laboratory to be able to send information from one place to another, this notion of being able to take the information and push it out there so that someone else can receive it. So it seems like the exchange for treatment or payment purposes sometimes, well, I should say, with regard to meaningful use. What we do know is that oftentimes this is going to be something that falls under treatment or payment purposes. Usually you are going to know the person on the other end. You know, it's to a particular person or to a particular pharmacy. And although, in some cases, there may be prior relationships, if it's a new consultation of a new prescription, the sender may not have that prior relationship, and so we want to make sure that we understand how the technical and policy framework can help support these kinds of functions.

If we think about the Nationwide Health Information Network, we've reviewed this in some of the previous meetings, but there are sort of six foundational components, so we talk about vocabulary, document, and messaging standards. Many of these have been articulated in the recent standards IFR. The last meeting, we talked a bit about directories and how those can support this, and I'll spend a little bit of time reviewing some of the recommendations in the discussions that we had at the last meeting. Today, our focus is going to be on authentication and certificates. And we also recognize that delivery protocols, security and trust relationships are also important components and clearly will be touched upon, I hope, in the discussions today since authentication and certificates clearly involve some of those things.

I think it's important to recognize too that the work that's going on here is part of an evolutionary path that we are moving incrementally towards the goals that we have for 2015, and that we're starting out trying to make sure that we start incrementally and can build on that, and part of these discussions is how can we take something simplified to make sure that we can meet the goals of meaningful use, but still with a look towards the future and some of the other things that are coming down the pipe. This gives you a sense that in 2011, we want e-prescribing, laboratory results into electronic health records and the exchange of key clinical information for patient care, as well as for public health reporting.

Incrementally, as the years go out, we will get additional recommendations from the HIT Policy Committee that will include additional kinds of data exchange, and that by 2015, we hope that there will be access to comprehensive patient data and the ability to do real time surveillance. And we will be working, I think, very closely with this committee and with the policy committee to help us achieve those goals.

With regard to the findings, I have just a couple of bullet points here that was an attempt to summarize some of the discussions that we had at the last meeting. What we found is that there are extensive provider directories out there, but there are a lot of different business models for which they were created, and it's not particularly clear that all of those are going to be sufficient to provide the kind of care coordination that we need.

Different directories have different kinds of data. There are different levels of data accuracy depending on the use and sort of the incentives for keeping them current. Different definitions of data exist, and there are certain kinds of data that may be needed, but may not currently be collected. Incentives must be sufficient to get the data needed for the particular purpose, and we want to make sure that the use and the necessity leads to appropriate checks and balances in the data quality, and that's going to be an important aspect to try to make sure that the data that people are using is accurate and is able to support those needs.

We also heard that the privacy sector and government programs that rely on directories will still need to maintain and operationally support those directories for the purposes that they've been initially set up to do. As a result, there is likely the need for policy standards and governance for directories in order to expand the exchange and collaboration and help those directories support the meaningful use criteria that have been identified by the policy committee. We also have to be cognizant that patient confidentiality and security are important because directory services, if improperly set up and offered, may actually increase the risk of identity theft, and so we need to think very carefully about making sure that that information within the directories are adequately protected, and that safeguards exist for that information.

Finally, we heard that there are a lot of different approaches that could be explored as part of our work going forward. These include having the federal government serve in a coordination role, perhaps setting up standards for a set of core data elements, creating authoritative directories or directory of directories. Creating certification based upon certain policies for data accuracy or timeliness, and these are the things that need to be explored. I don't think any of these have been decided upon, and we certainly are going to be looking to this committee to help us with some of these things.

Today the goal is really to focus on authentication, and so the question is what can we do today to accelerate information exchange under a variety of different scenarios, and what are the issues related to authentication that can help accelerate that? In supporting near-term functionality of exchanging and supporting meaningful use, as well as some of the broader NHIN query functionalities. We need to focus on the need for authenticated entities, individuals or organizations, and there are lots of different models to think about. One is sort of a delegated one in which organizations maintain that. Some can be at the individual or the provider level, and I think this is a time where we'll have an opportunity to discuss different authentication models, and get some testimony from folks about what has been done within federal partners, as well as in the private sector.

Other considerations for the committee include the need for what we call a solid trust fabric, the ability to sort of have trust as part of the exchange of this data. We hope that you can provide us some clarity around what is the best role that the government can serve in this, and that, at the end of the day, we wish to enable broad participation across the spectrum of organizations from both very small organizations to large ones as well. And so, with that, I'm going to go back to the agenda. We have testimony, I guess, next from Dave Riley. Has he…?

Judy Sparrow – Office of the National Coordinator – Executive Director
He's on his way.

Doug Fridsma – Arizona State – Assoc. Prof. Dept. Biomedical Informatics
I'll turn it back to David.

David Lansky – Pacific Business Group on Health – President & CEO
Just one other comment just comes to mind, Doug, with your presentation. I think a number of us understand that over that arch of time that Doug described, the scope of authentication requirements or the scope of the population who will be interested in authentication will grow from the immediate, the inner circle, if you like, of eligible professionals and hospitals, and maybe the immediate participants in meaningful use, ultimately to the entire population. I think, as we are framing the problem at this stage, primarily as one of provider-to-provider data exchange for the purposes of 2011 and so on. At the same time, we know that in 2013 and 2015 and beyond, there are a much larger number of much less well-organized users who will be interested in sharing health information across the nationwide network.

To that end, I hope you'll help us understand where there are solutions or policy issues that you have worked on and addressed that speak to the professional and institutional data exchange. Are they going to extensible and scaleable to the general issues in the population, or do we need to be thinking about a roadmap that accommodates this much larger set of issues, as you think about the whole population being users on the network. We don't want to solve that problem today, but we also don't want to close off doors that are going to get us there in the next four to six years, let's say.

While we're waiting for David to be available, I wonder. Any of the committee members who have listed to Doug's presentation or otherwise in pondering this have any other comments or questions you want to surface for us or for the witnesses today? No? You want to start the federal panel? All right. We'll do that. Those of you who are participating on the federal panel – David, Tim, Peter – are you available now? We could get started. I'd ask you both to just take a second and introduce yourself and maybe just a moment of your background and role, and then also if you could make an effort to limit your verbal comments to no more than five minutes, then we can have time for a discussion with the full group. Again, thanks very much all of you for coming, and please take a seat. Why don't we start with David first, if you'd mind just introducing yourself and then jumping in?

David Temoshok – General Services Administration – Director
Thank you, and I'd like to thank the Health IT Policy Committee and the working group for inviting us to submit testimony, as well as inviting us to make comments here this morning. I'm David Temoshok. I'm the director of federal identity management for the GSA Office of Government Wide Policy. In this case, we're charged with the mission of providing for the federal government the infrastructure – I'll call it the program – for how we, as identity providers, manage identities for our employees, contractors, other

individuals that are accessing our systems and our facilities, but also how we authenticate the public for our electronic government purposes and for our business purposes in the federal government.

You have testimony from Judith Spencer from my office in your packet. I will be addressing some additional comments. I'd like to elaborate a little bit beyond the responses to the questions in the testimony for our mission and how we've gone about it. Our mission for the federal government, I think, is not dissimilar to the mission that's facing this working group, as well as the policy committee. We were charged with providing for common infrastructure for the authentication of our internal people, businesses coming to do business transactions with the federal government, as well as the public: the U.S. national public and internationally, how individuals, businesses, and organizations would access our protected resources in an online process, conduct transactions with us, and support our electronic government applications in the federal government where authentication was necessary. Where it was necessary to know who it was on the other side of the transaction coming in.

We were charged; we've been charged with this since 2001. My office in the General Services Administration has had this mission since 2001, and I'd like to make a couple of points about how we've gone about that for the federal government, which I hope will have relevance to the working group. First of all, our infrastructure is based on a common policy framework in the federal government, both my office, the Office of Government Wide Policy, the Office of Management and Budget, and most recently under the CIO Council, a government wide governance body called the Identity Credentialing and Access Management Subcommittee under the CIO Council have the responsibility for issuing government wide policies for how we do authentication. And I'm not going to go into all of those policies, but I would like to mention three key principals.

First of all, you may hear mention throughout this morning of the federal government's policy for authentication levels of assurance. In 2004, we, with the Office of Management and Budget, issued what's called OMB Policy Memo 04-04. What that said was there's not just one way to do authentication with one strength. But in fact, we defined four levels of authentication assurance based on the risk associated with the access to the resources or assets or the transaction that's being performed. Defining the level of authentication of assurance that's necessary, and tying those to four defined policy levels.

Secondly, our policy was built around that we would leverage identity credentials and identity management practices outside of the federal government, that we were not going to be issuing national IDs or IDs to everyone and everyone and every business, but rather that we would leverage the infrastructure that already exists in different communities. But the third key policy point on that, in leveraging that was that we must be able to trust the identity management practices of other organizations and have a means to establish that trust, and we must insure that the authentication processes of organizations that we would be using outside the federal government or across the federal government are interoperable in how we exchange data, how we process that, and the definition of that data, which are used for identity authentication assurance.

In order to implement the policies of the federal government, our identity management policies, we looked to standards, industry-based standards for both the technologies, as well as the protocols. And we want to use mature technologies. This will not be a technology discussion. But we've adopted a number of authentication technologies, as well as protocols, and when we adopt those technologies and protocols for federal government use, what we then do is define exactly how data will be arrayed, what that data is, and how it will be transferred, whether that transfer is across devices, components or systems, so that specifications for the federal government's use of industry standards to implement our identity management policies are put into place. Consider those interface specifications for how data is exchanged. Without that, we cannot have interoperability.

The third point that I want to make on our program is about trust. In order to insure that entities within the federal government who are issuing IDs, issuing identity credentials, and managing identity for our employees, but also for entities external to the federal government that we want to trust. We build the standard trust model. That standard trust model is based on the four levels of assurance from Policy M04-04. That level of assurance, we asked our friends at the National Institute of Standards and Technology to elaborate on the policies for those four levels of assurance. They did in special publication 800-63, which defines both technically and from a process standpoint how entities would conform to our policy requirements for levels of assurance.

We take those requirements from the National Institute of Standards and Technology, and we built evaluation procedures for different protocols, both for how we manage identities in the federal government, but also how external entities that want to interact and interoperate with us in the federal government and be trusted can be evaluated. And we established committees within the federal government to provide that evaluation and approval process, so we lined up with trusted entities within the federal government, trusted entities outside the federal government that have been evaluated to conform to both our trust requirements, as well as to conform to our interoperability requirements for the profiles that we've written.

The last point I want to make on our program is, I've described what the federal government has done in establishing the program for policy based framework, industry-based standard implementations, the trust model for evaluating identity providers within the government and outside, as well as how we determine and conformance with interoperability requirements for any protocols. The last point I want to make is, we've defined additional roles for industry. That this is not exclusively the federal government that does this. Certainly, establishing policies is the federal government role, but when we look at how trust can be generating and evaluating identity providers against established criteria, that's not necessarily a federal government role, and we've encouraged industry to build the capability to provide that function, both for us and the federal government, so that we can trust industry-based providers or commercial providers or other organizations, but also how that same framework can be extended beyond the federal government for other purposes as well, for other communities, whether those communities be healthcare, emergency responders, or higher education. In that way, there's value to both us in the federal government for our electronic government program and the online functions that we perform, for the providers themselves in expanding the scope of their trust, as well as for the users of those communities in building a trust framework that they can use their credentials, their processes for both external use and internal use for us in the federal government.

I'm happy to take questions at the end of the panel, and I will turn to our next panelist, Tim Polk.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks very much. Welcome, Mr. Polk.

Tim Polk – NIST – Computer Scientist
Good morning. I'm Tim Polk from the National Institute of Standards and Technology, and I'm very pleased to be able to come. Thank you for the invitation, so I can come and give you NIST's view on authentication.

I apologize. We did not have – we have some competing interests going on at the shop right now, and we did not have time to get written testimony together, so I'd ask your indulgence to give me a couple of extra minutes because there are two specific efforts I would like to describe that I think will be of interest to you.

M
…most of my time.

Tim Polk – NIST – Computer Scientist
I think I was getting the OMB time as well. The first thing is, at NIST, our authority is limited to non-national security systems, federal agencies, federal data. That is the scope of our authority. However, I should say that adoption or convergence, adoption by or convergence with private industry is a key metric of our success. When we build standards that no one else wants to adopt, we know we haven't done them very well. So there's a difference between what our scope of authority is and the scope that we hope to address in our efforts.

Authentication, I think, as David alluded to, in our view, it's a lifecycle. It's not just a protocol or a mechanism. It begins with determining who someone is when you establish them as part of the authentication system, tracking them, and removing from the system when you should. It's not just the protocol of the bits running on the wire.

With the two efforts that I'm going to talk about, they both are focused on identifying who the person is, not at all with authorization. When I looked at some of the – I think the definition that this workgroup may have adopted for authentication may be broader than what we have looked at. We certainly draw the line in both of these efforts before the authorization step. We see authentication as being the foundational element. If we don't know who you are, how can we decide whether or not you should have access to data? But the efforts that I'm talking about leave authorization as a local decision. This is to give you the information upon which to make that decision, but to go no farther.

As I said, there were two very different efforts that I want to talk about. They come from trying to solve very different problems. The first one that I would like to talk about has already been mentioned is the 800-63 work, which is actually responsive to OMB 04-04. There, there was an establishment of a set of four different assurance levels, and there was a requirement placed upon NIST to go and write technical guidance on how to implement and achieve those four different assurance levels.

The interesting thing about 800-63 within that is that because we are trying to solve a very great range of problems from the lowest level where all we want to do is be sure that we are tracking the same individual, we really have no idea who they are, to one where we have very high insurance up at level four. And where we could not prescribe exactly an architecture, that document is more of a framework. It's built, for example, to permit delegated authentication, but it certainly does not require such a model.

Many of the techniques that are described in 800-63 permit the use or might even require the use of directory services, but there are others that would be completely independent. 800-63 was designed with the idea that we want to be able to authenticate citizens using whatever credentials they may already have in place, and we're looking for ways to leverage those kinds of credentials, not necessarily mandate that these credentials be issued by or directly on behalf of the federal government. That's a very broad range of trust problems.

The second effort that I want to talk about is FIPS-201. The FIPS-201 personal identity credential, a verification credential, was specifically targeted to be responsive to Homeland Security Presidential Directive 12, which has the goal of being able to strongly identify government employees and government contractors. In this case, it made sense that this is going to be a credential issued either by or at least on behalf of the federal government. Here we were able to take a much more tightly prescriptive approach and be able to specify the technologies and actually target particular levels of assurance that we wanted to be able to get with the different aspects of the credential.

That's the case where we actually do require directory services to support certain parts of that. It's also a place where the delegated authentication model is assumed. Federal agencies should be able to authenticate credentials that come from other federal agencies. So that kind of is a quick and broad overview of what we are doing at NIST.

One thing I would like to add to that is that in one of the more slow rollouts, unfortunately, of all time, we are working on a revision to 800-63. 800-63 was originally written to be very prescriptive and make it easy for federal agencies to implement, although limit their choices. So there's a tradeoff between giving choices and making it easy to implement. The initial versions of 800-63 were intended to take the mystery out of the process, but not permit all possible authentication mechanisms to be employed.

Based on the feedback that we've received from industry and from agencies, we have been working to broaden that approach and provide more flexibility to agencies in meeting the mandates from OMB 04-04. There has been one public draft that has been released. There is a second public draft that will be coming out. I certainly hope it will be this month, but if not this month, I really hope it'll be next month if it's not this month. But we are working to move that way, but it's been a very difficult problem to walk the tightrope of making this accessible and implementable by agencies, and yet not overly constrained. And so there are versions of that document that are already out there. We continue to try to improve that, and hopefully that will be available to you in the next month or so.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks very much. Dr. Alterman?

Peter Alterman – NIH OpenID Project – Assistant CIO
Good morning, ladies and gentlemen of the committee here. It's a pleasure to come down to the Mayflower first thing in the morning and get warm. Someplace that's a block from a metro stop is always welcome.

You've heard from my colleagues. These are highly valued colleagues that have worked together for many years. You've got my written responses to the questions, so I don't want to rehash that, but I do want to make a couple of points.

The first point is that the questions and issues, which you are concerned with, are not new. The questions and issues that you are concerned with have been churned for many years, both in the private sector and within the federal government. Within the federal government, starting in 1998, I have been involved with the activities related to solving these problems, and they were going on many years before I showed up. These have been addressed in the technology, policy, and practice dimensions, and solutions have been in place, both at the policy level and the practice level and, as David mentioned, the technology level, in production for several years.

Therefore, I do believe, and I strongly encourage you to not create anything new, to not ignore what has gone before, but to fully inform yourselves with the existing environment that is critical to your success in both the short and long-terms. One of the reasons it's very important is because the fundamental conceptual model of relying on credentials issued by other entities at known assurance levels is fundamental. It is very important. That links your applications to other people's credentials. It works on a baseline of mutually agreed upon trust.

Not only is this something, which is operational within the government from both the perspective of credentials issued under both the FIPS-201 model and other models, but it also has been widely adopted in the commercial and the private sector. We have very strong, long-term relationships with many of the credential provider, the technology providers, the credential implementers, and I want to say the OEMs, the software solution providers who run and build software applications on behalf of the federal government.

Many of our partners and colleagues in the private sector are behind us today, and they can testify to the success of knowing what to build to in order to have a successful product and service provided in the marketplace. The goal has been to do together what we can't do separately. To rely on credentials issued by others at known levels of assurance using all available technologies. That's what David's program has been all about. That's what Tim's practices have been all about.

When it comes to the National Institutes of Health, of which I am happy to be a long-term pee-on, we have implemented the trusting party piece of that very aggressively. We are capable of and in production today do rely on credentials issued by many different parties at known assurance levels. We have tens of thousands of university credentials coming to us to access NIH applications electronically. We're able to validate them, and we're able to pass the assurance level and the validation and the identity credential to the relying application. The NIH library is a classic example, but only one of many. Electronic Research Administration is coming online, so we're going to be able to do electronic grants in a much more robust fashion very soon.

There are certainly within the federal government, upwards of 20 million employees, including the military and in-house contractors, have high insurance fixed to a one compliant credentials. I have one in my pocket. It glows when I turn off the lights, and we're able to use that to access doors. In my case, I can get into the mouse labs and not be arrested. That's an exciting option, and also to authenticate to my electronic infrastructure, to my network, to my electronic personnel folder, to my travel system, to my e-mail. These are very important, high risk, high assurance activities.

The credential, the high assurance credential allows us to do that. But I would assure you, well, my partners will speak for themselves. I assure you that this is the high assurance, we know what your DNA is and where you park your car, level of authentication is not necessary for all applications, perhaps not even most. Frankly, I don't know how urgent it is for everybody to know with a high level of assurance that I'm wandering the mouse labs, but there it is.

There are solutions in production now at all assurance levels – one, two, three, and four – using a wide variety of technologies, using the SAML technology that higher ed uses with Shibboleth, the OpenID solution, Info Card, digital certificates, one-time passwords. We have all of these in operation in production. Clearly the model that the government has put together has been a model that we have been able to use. Thank you.

David Lansky – Pacific Business Group on Health – President & CEO
Great. Thank you all very much. Let me turn to our panel, and also those of you on the phone. We want to just check in again. For committee members who are on the phone, I think Marc Overhage may have joined us and Marc Probst. Anyone else on the phone? Okay. Let me ask my colleagues if they have questions of the panel. Arien?

Arien Malec – RelayHealth – VP, Product Management
I've got a number of questions. One, just relating to the last points you made, if you can testify as to levels of assurance at inflation, that is, the notion that everyone believes their need is slightly higher than

everyone else's need, and how you are able to or if you're able to get sort of downgrade levels of assurance. You gave the example of the mouse lab.

Peter Alterman – NIH OpenID Project – Assistant CIO
Yes. Well, after some raids from some animal rights organizations, we felt that maybe the mouse labs were something we needed to protect a little more, but fundamentally the guidance of MO-404 is paramount for us in the federal government. But broadly speaking, the principal of using or applying a standardized risk assessment methodology to your online application is what churns out your assurance level. The federal government has a standardized methodology that they contracted with Carnegie Melon University to develop for them. It's been on and off in revision for a while, but it is a really solid place to be.

So if you have an application that you want to put online, or you have a system of applications that you want to put online, it's incumbent upon you, and it's mandated in the federal government that you do a standardized risk assessment. One of the outcomes of that standardized risk assessment is the information about what assurance level you need for various roles. So if I'm just the user of a system, I only may need a level two credential to access it. But if I'm actually going to change data, I might need a level four.

M
I just would like to elaborate on Peter's response in that our mission was to be able to provide the authentication tools and infrastructure at four levels of assurance for the federal government's purposes in a standardized fashion. The decisions for authorization based on whatever level of authentication is determined needed by the owner of that application is their decision. We did not try to standardize that or dictate that, but to allow the tools, based on risk-based decisions, and Peter mentioned tools that we've provided to allow the determination of the risk and vulnerability for their online applications, but the decision for what level of assurance was necessary for authentication was the application owners.

M
If I could add one thing to that, the real importance of using the tools is that there are two mistakes that people will make if they don't rely on the tools and work, you know, really do the method for risk management, risk assessment, and determine the level. The first one is that everyone believes that what they work on is very important, and so they all believe that it must be level four. That's the first reaction that we sometimes get.

The second reaction that you sometimes get is I already know what technology I want to use for authentication, and so my risk assessment has to come out at level X because that's the highest level that my technology will permit. So if you let either of those overriding concerns derail you, you will either spend too much for authentication because you didn't need level four, or you won't get the security that you need, and you'll be sorry farther down the road because you came into it with a decision made upfront. And so, as Peter was saying, running the tools, there's a lot of background and history, and relying on those is an extremely important piece of getting it right here.

Arien Malec – RelayHealth – VP, Product Management
The second question that I have relates to actually the point you just made, which is the cost and utilization tradeoff between levels of authentication. That is, first of all, any data that you have on the cost tradeoff, but then also in areas where the utilization of the system is quasi voluntary, whether you've done any research as to the utilization tradeoff of the levels of authentication. The reason I'm asking is that a physician, there's a tradeoff between making the system easy to use so that we get more information

sharing, and requiring higher levels of authentication that may end up putting barriers in the place of utilization.

Tim Polk – NIST – Computer Scientist
From the point, let me take this one first. From the point of view of 800-63, utilization was not actually – you know, it was strictly risk security, can we achieve the level of assurance. We recognized that there is certainly a deterrence when it's voluntary to adopt them, and we have really searched, especially in the revisions here that are ongoing for ways to incorporate more cost effective, more user-friendly technologies. It's a really hard problem. As the security requirements, the assurance requirements go up, and privacy issues, everything else goes up. It's very difficult not to make those higher levels become more difficult.

Now utilization might be something that you can choose to factor in, in terms of your own decisions. It wasn't a degree of freedom that we had from OMB 04-04, but it certainly is a factor in whether or not some of these projects are successful. We've had the luxury with something like FIPS 201 in that it was not an opt-in process.

M
I would like to elaborate a little bit on Tim's response. As with any security mechanism, when we define levels of assurance, as the security level or the assurance level increases, the cost of the security mechanisms will increase. For what we did for the federal government in response to Homeland Security Presidential Directive 12, and what's been referred to as FIPS 201, the standard for a standard government ID, the credentialing, and how identity is vetted and bound to that credential, we define the highest level of security. We also allow, in use cases, lower levels of authentication if that's using that PIV card and credential, if that's what the application owner needs. But, nevertheless, there is certainly a cost, and there's a cost to the infrastructure and the use of credentials that are facing your working group.

I'd like to reiterate the point that Peter made.

By establishing common policies, common standards, and common requirements across the federal government, what that does is organize the market so that developers and service providers, product developers and service providers are developing products and services to conform to a common set of requirements. Not many different requirements at a cost to the developers and a cost to the consumers, but common requirements that can meet and conform and maybe exceed our security requirements at a cost that becomes affordable to us and cost effective in the federal government, and to our users, as well as to the industry providers. That organization of the market becomes very important, as we look at communities that are adopting the high level of security that we've defined under FIPS 201 for their own credentialing, recognizing that that's market driven, and we're driving both the security level, but also the cost structure, and the ongoing delivery of those products and services, as we go forward.

M
We have not yet seen a use case in this space, and we've talked with many of your government-wide colleagues. We have not yet seen a use case where we don't see we haven't, together, around the table, been able to find a cost effective, user-friendly solution that accords with 800-63 and 04-04.

M
Thanks. I have….

M
One last point: I just realized something. There was something important about utilization I should have noted that when you factor in utilization, part of the question will be is the person opting in also the person whose data is being protected. And so, in the case where we want the doctor to utilize the system, but yet the data that we're protecting is the patient's. That's a very – again, it's a tricky question, and it's one that we're actually very happy we didn't have to address in 800-63. But it's something that I'd like you to keep in mind if you do decide to factor that in.

David Lansky – Pacific Business Group on Health – President & CEO
Carol, Farzad, and Wes so far.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I want to get to the issue that you all kind of raised as the necessity, which is this reliance on third parties. There's no way to make the system work unless you can bootstrap on existing credentials. And shift to the issue of the oversight mechanism to make that work, and I know there are documents that NIST has done on sort of the ongoing monitoring policies. But I'm interested in particular if you could elaborate for us and help us understand how you do this in a more detailed way.

In other words, are these third parties observable in any way across the network? And what's the policy around audit and redress and some of these issues, because I think it's one thing to say we have a certain set of criteria, and we're going to test and make sure you can do this the first time. It's another saying if you want to maintain trust, to police across the network in an ongoing way and make sure that any inconsistencies are observable to everyone who is relying on that trust framework.

M
We all look at each other and say, well, you know…. In fact, the federal government has a very robust program in place that does this. It kind of works in general services administration. It's the locus of the actual effort. There … high assurance cryptographic, it's the federal PKI policy authority, which not only evaluates the policies and practices, both business and technical, of high assurance, cryptographic providers who want their credentials to be utilized in the federal space. That requires an annual audit by a third party, an independent third party auditor. So the government gets an annual report on whether or not that credential provider is living up to the policies and practices that have been assessed by the government. That's a very rigorous and robust and, frankly, expensive process. That's for cryptographic level three, level four credentials.

At levels one and two, the requirement for oversight and audit still exists, but because level one credentials are basically little or not assurance of identity, the audit requirements, the assessment requirements are much less rigorous. At level two, they become more rigorous. At level three, they become substantial. Level four, they become almost onerous. So there's varying degree of oversight, varying degree of review depending upon the trustworthiness of the credentials by definition.

At level one, there is no real requirement for audit, but there is a real requirement. You could speak to this better from 800-63. This is all codified. GSA has a program that assesses credential providers and trust framework providers, which are consortia, federations of credential providers who operate under common practices. And there is a standard methodology. It's published. It's been reviewed. It's been blessed by the Federal CIO Council, and that practice, that methodology describes how the federal government assesses candidates who want their credentials to be trusted and utilized at federal sites. That's in production. That's been in place for well over a year and a half now at levels one, at level two, at level three non-crypto and, of course, level three, the three crypto and four have been operational very successfully since 2001 in the federal space and commercially as well because there's been broad uptake. As David mentioned, we have had a strong impact on the market in all assurance levels.

I also want to say that the methodology addresses questions of privacy, so that not only do we want to be concerned about the trust level of the credentials that we're seeing from external providers, but we want to know about their privacy practices. We want to make sure that they conform with minimal government comparable privacy practices with relation to the individuals who are using their credentials at the government sites.

M
Let me provide a little more insight on why strategically we did this. That determination of trust, an external third party's identity management practices, how that trust determination is made becomes very important. We determined in the federal government to centralize that evaluation process in my agency, as well as inter-agency committee structure where we do that evaluation process. If we didn't do that, each agency would be up to making those determinations on their own, obtaining whatever policy document, procedural documents, maybe audits that may be performed, and attempting to go through that to determine is this entity somebody that can be trusted.

We felt that it's much more effective for the federal government to centralize that function, publicly post our evaluation procedures, our requirements, and how we go about that process, as well as the entities that we've approved as trusted entities so that other communities outside the federal government – the federal government is required to use those providers. But so that communities outside the federal government could see our process, and if they trust what we've done, they could accept our trust determinations.

I think that it becomes very important in considering how that trust is built to a point that I made in my comments that we're encouraging industry to perform some of those roles. We publicly post our requirements, our criteria and, in fact, we published documents for how industry could actually make those determinations, those assessments, and demonstrate to us their process. We call it federation trust providers for how those determinations could be made, so we could rely on determinations that are made within that community, by an entity that has the authority to make evaluations and make determinations with the idea that we, the federal government, don't have to go out and evaluate everyone. That there would be benefit across both government and industry groups to common practices and a common trust model. We would like it to be the common trust model that we built for the federal government because that's our policy basis.

David Lansky – Pacific Business Group on Health – President & CEO
Carol, go ahead.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I just want to ask a follow-on to this. I understand that piece of it, but is it true that the way the third parties perform against those requirements is observable across those parties, and also, is any inconsistency observable across those parties? In other words, if you want to establish the trust across the network, it's important to let other parties know that although we initially evaluated this entity as a trusted partner, we've had some experience that indicates that that may not hold true any longer.

M
Certainly at the higher assurance levels, there's an annual, independent audit of practice, which does catch that stuff. There are – I don't want to make bad jokes about audit firms, but in fact we rely on the reports of independent auditors who review the practices of high assurance credential providers, and they are required to report to the federal government annually, so we have a very good view at that.

At the lower assurance levels where the risks are lower, the audit requirements are less strict, but they do exist. Even at level one, there are requirements for an annual report on operations and practices. Where we get reports of problems from either individuals relying parties, software people who have said, well, I use this credential and it blew up. We have mechanisms in place in our memoranda of agreement with the credential providers or the federation of credential providers to request review and information about what's going on so that we can explore challenges when they are brought to our attention.

David Lansky – Pacific Business Group on Health – President & CEO
We have about ten minutes left, and I'd like to see if we can move on. A couple more people have questions. Farzad, then Wes, and then others, go ahead.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
What is the minimum that this workgroup needs to do to enable a million health providers across America in a variety of settings to be able to engage in secure, authenticated health information exchange?

M
I think you heard a consistent message from the panelists in that we've described the federal government's identity management program on how trust and leveraging third party credentials have been implemented in the federal government. The minimum that we would recommend is the workgroup familiarize yourselves with the models that we've discussed and bring that to the Office of the National Coordinator.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I'm looking for something a little stronger than that.

M
All right. Well, clearly I would say, based on what we have seen, that one of the things, which is paramount to your charge is that the citizens who are in this system, who will be in this system will be able to trust it, trust it with their medical records, trust it with their personal information. And so it is extremely important that this process, that this system that you are considering be trusted by the people who have to use it. In order to do that, there are standards and guidance's already in place.

The Privacy Act is a good model. The Privacy Act says that if you are going to exchange personally identifiable information electronically, you have to protect it at the OMB assurance level three or NIST assurance level three. There are a number of technological solutions to doing that, and those technological solutions are also varied by requirements for implementation practice, so it's not just about whether it's one time password or PKI. It's about how you implement. Level three does allow a great deal of flexibility on how you implement, and I would strongly encourage this committee to accept nothing less than level three.

David Lansky – Pacific Business Group on Health – President & CEO
You have a follow-up?

M
Yes. A couple of quick things that I'd like to add to that, one thing is although … just to reiterate, and it's probably not what you want to hear that because of your aggressive schedule, I mean, I was looking at what the timeline was for the different applications you want to have come online in 2011, 2013, 2015. It's essential that you go for refinement of what exists rather than an invention of something new. And so I think that's going to be important.

Another piece is, even in that short a period of time, my experience from 800-63 is technology moves fast. Rather than focusing on what the technology should be, I believe that focusing on what are the real risk levels is probably the most important thing to do, and then maintain your technology independence.

The one last piece is that what I think that we have found in the past is that people want to drive an entire system up to the high watermark of the level of assurance. Where it's frequently true that you could build a system where many of the users can work at a lower level of assurance and only certain things have to move to the highest level of assurance. And avoid the drive, as we were talking about before, the inflation point, and try to break out the applications into buckets rather than one size fits all, I think will be very important to be to success.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Let me try this out on you. What if – is what you're saying in a more maybe politic way than you are prone to speaking, is what you're saying to us, listen, what you guys have to do is you have to either announce or put in place a process for stating what the level of assurance is for various roles and uses, use cases for the National Health Information Network, or for anything else, anyone else who wanted to do this, right, whether it's, you know, whatever railroad wanted to do this, right? It doesn't matter. Figure out what the level of assurance is, state it, and then anyone who wants to participate could go to any provider of credentials. And a convenient way might be those that are accredited by the government on your list as being able to provide those assurance levels, and you're done.

M
I would claim that from what you've said, the one thing is that even within healthcare, there will be applications that have a range of levels of assurance. Driving this all to one level of assurance will force you to the high end. So it may be that there are – it may or may not be that there are no applications that would match up to what OMB 04-04 calls level one, but there may in fact be times when you only care to know that it's the same patient, and you don't need to know who it is, so there'll be some range of levels, but what is important is that regardless of who I choose as my healthcare provider or who is my insurance provider, that they use the same metrics to determine how to protect my information so that they can do the same risk assessment because you do want that continuity, and I don't want to have to ask when I am going to a doctor. Do you use that method of determining how to protect my data or some other method? I think that's important to bring some—

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Right, but in terms of what I said, our job is to set in place a process to determine what the level of assurance is for various use cases, and then telling folks, go find a provider who will do that level of assurance and that is part of a larger accreditation process.

M
Part of your mission is to accelerate the process. That would accelerate the process and your implementation.

M
I think it would be an important step forward.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you. I think we have Wes and then Jim, and then we'll probably be out of time, and we'll still try to come back to David Riley's overview at that point.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Thanks. I want to thank Dr. Alterman for getting down to brass tacks and talking about how many people are already doing this, and what I head was tens of thousands of people in the university environment. Is that right? Okay. We're talking about a challenge, as Farzad noted, that's roughly a million people, most of them, certainly the majority of them working in organizations that have the IT competence of a corner grocery store. And, therefore, I need to understand a little bit more.

I get confused by the different organizations that we've talked about this morning. There is the organization where the user works, and presumably gets their IT service from. There is the organization that issues the credential, and then there is—

M
…not be the same.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Which may or may not be the same. All right. Then there's the organization that uses the credential, that relies on the credential in order to grant access to some resource. So the level, sort of the non-mechanical, it's something I have, that sort of thing. I use this wiz bang versus that wiz bang. Forget that stuff, but if I know that this is Dr. Smith, what do I need to know about the place that Dr. Smith works in order to grant a level of assurance? Do I need to know anything about their security practices? Do I need to know about their employment practices? Do you expect the credential issuer to have ascertained that about the organization before issuing the credential? Thanks.

M
Let me speak from the point of view of SP 800-63. We don't make assumptions about whether or not your desktop system runs anti-virus software, whatever. Those things are considered to be out of scope and really something that can't be verified, that they are left out of it. That's why what you'll find is that as the levels of assurance move up, we rely on credential form factors that are separate from that desktop system or that laptop that that person uses, and the protocols that are used, which is something we really didn't talk about, but also become more complex so that they basically provide a secure channel between the device that's being used to authenticate and what we call the relying party who's trusting the credential. So it becomes less about the facility where they work. That's not something that we really think is probably – you know, accrediting the IT shop at every small doctor's office is probably not doable. However—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Or necessary.

M
Or Necessary. However—

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
…level three?

M
So even at level three or at level four. At level four, we actually have very strong requirements that you use hardware credentials and things, but there are some problems that we can't solve in the standards. And the fact that the IT shop may not be very good is one that we punt on. The idea about whether or not

the credential provider we put much stronger requirements on because if in fact that IT shop is not very strong, we don't want them issuing the credentials anyway. We want you to go to a third party provider who actually makes it their business to do this and do it well, and so the design of things like 800-63 was designed to move that or to remove that question or simply not to rely on the answer of whether or not that local IT shop is, you know, what the level of quality is there.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Okay. So just to make sure I understood because scope … here, your approach for at least up to level three authentication is to use technologies that are relatively immune to poor security practices in the system where the authentication occurs, and that it's a relative….

M
No, I think that what we would say is that as the levels of assurance are increased, we're using technologies that provide greater protection, even in the face of some of those threats. At the lower levels, we certainly would make no claim that someone whose computer has been taken over by malware is in any way protected against having their private information leak or losing their authentication credentials. We simply are saying that at those levels, it's a risk that we're actually willing to take.

M
Because the downside is so small.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Sure.

M
Right.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
And just to confirm, we've been talking about the policy necessary to be sure of the authentication of the person, nothing about protecting the information after you've authenticated.

M
Absolutely, but OMB 04-04 is all about the ramifications if information is disclosed, and so we certainly are thinking about those ramifications when we determine which mechanisms are acceptable at which levels.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
One last question: Is the recommendation to go to level three more or less the equivalent of saying that we have to have the doctors offices practice FISMA level? No?

M
Not at all.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Why not?

M
Those are separable issues. I said I recommended level three for protection of personally identifiable information because that's what our model requires of us. If you are a doctor in Spearfish, Montana, and

all of the IT you have is a couple of desktop machines and a laptop, we are not looking at how you operate those machines, whether you do anti-virus. We're not looking at that.

What we are looking at is an electronic credential at level three, some technology that has been issued in accordance with policies and practices. It has been issued by an issuer who conforms to policies and practices that align with 800-63, M04-04, and some of the privacy requirements. That's all we're saying. Some of the issues you're touching on, I think, have to do with attributes of certain individuals, and that's a whole other panel presentation. I'd be happy to come back and drink beer and discuss that.

M
But just to point out on the roles, if we identified the role of an identity provider that manages identity, vets identity, verifies identity, and issues a credential and a relying party, we centrally evaluate the identity providers, and part of that at the higher levels of assurance is how they assure that their end users are using the credentials properly, and that includes protecting the credentials, so that that determination of a trusted identity provider that our relying parties can than trust. They've gone through a vetting and evaluation process from the federal government so that that identity provider can be trusted, and the users of that identity provider and their credentials can, therefore, be trusted.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Would that imply then that somebody who is certified to issue a level three authentication would have to go out to Spearfish, Montana, and visit the doctor to see how he's doing?

M
No, 800-63, if we use that as the baseline, permits remote authentication up through level three. Now it puts a number of additional requirements that leverage some other things we trust like postal delivery and that sort of thing. It doesn't allow instant gratification, but we don't mandate that either the doctor leaves Spearfish or anyone go to Spearfish until you reach level four.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But David said they had to assure how they used the credential and kept track of it as opposed to simply how they got it issued in the first place. I'm wondering if that requires a visit to Spearfish. I hope the Chamber of Commerce is listening.

M
There are no roaming vans of assessors going through the country checking….

David Lansky – Pacific Business Group on Health – President & CEO
I think we'll have to suspend this part of the conversation and come back to it later. Jim, you have one last question?

Jim Borland – SSA – Special Advisor for Health IT, Office of the Commissioner
I have a quick question related, and it's really related to something you said, David. You talked about GSA's relationships with businesses. I mean, obviously for contracting purposes, and I'm wondering if those relationships from an authentication standpoint, are they organizational level? Is there a model that supports organizational level authentication with a trusted organization?

David Temoshok – General Services Administration – Director
Let me explain that. There are product developers and manufacturers that are used in authentication systems. One of the things we do is approve the products that they in fact conform to our specifications and can be used. That's' at the product level. There are service entities that are contractors that do

work. It could be credentialing work. We also approve those entities. Where there are organizational entities that do their own credentialing within that organization, or they oversee a credentialing process, call it an identity federation where they established rules, much like we've established in the federal government, and are governing that.

We also allow for the approval of those entities as identity providers or identity federations, so we approve contractors, and contractors' products, and service providers for government wide use, but those approved lists are publicly available. And we also approve, not under contract, but under our identity management, we approve entities that have conformed to our policies as an identity provider, as well as organization that could do that, do the work to evaluate identity providers and determine their trustworthiness at a given level of assurance in conformance with our policies. We call those federation trust providers.

M
Right, and in a federated model though, the trust relationships still assume that, at the lowest level, individual identities are authenticated.

M
At the level of assurance that the credential is issued to.

M
Each level of assurance is level of authentication assurance for an authentication transaction.

David Lansky – Pacific Business Group on Health – President & CEO
Let me just ask if anyone on the phone, Marc or Marc at least, have any other questions before we wrap up this session. All right. Then let me thank you all very much for taking the time to join us. I'm sure we'll be talking with you more.

M
Thank you.

M
Thank you.

David Lansky – Pacific Business Group on Health – President & CEO
We might take just a minute and see if David Riley is available just to go back to the opening presentation, which we skipped over, and maybe we can compress it into just a few minutes given that we're a little behind on time. David, thank you. I know it's been a tough morning. Thanks for being here.

David Riley – ONC – CONNECT Initiative Lead
Good morning.

David Lansky – Pacific Business Group on Health – President & CEO
And I think, as you've probably heard, we've touched upon a number of themes in your remarks, so maybe you can just fast track us through a couple of the key points here.

David Riley – ONC – CONNECT Initiative Lead
Sure. We've only got three slides, so I think we can keep it fairly short, unless there are a lot of questions, so if we can jump to the first slide. What I was asked to do was to give a little bit of background about authentication in the NHIN as to where we are today and what we've been working on

over the last couple of years. I think it's important to articulate a couple of the driving principals that were involved in the process of building a solution for the NHIN in terms of the messaging security and privacy foundations services that we've defined so far.

Two of those principals, I've listed here: one is the local autonomy principal; the other is the local accountability principal. The way we articulate the local accountability principal is there are two aspects to it because there are senders and receivers of information in health information exchange. Basically the local autonomy principal says that the decision to release information is a local decision because care is local. It's between the provider and the patient. And so the people who have the basis for making a decision for the release of information are at the local level. We basically defer any decisions for the release of information to that level.

We also said that when you authenticate providers or users of your system within your NHIE or within your organization, whatever form it happens to take, that authentication levels are a local decision as well, so it's up to the organization, based on their risk analysis, to determine what the risk is to the information and the application that uses that information and the users that have access to those applications to determine what level of authentication is required for individual users to be able to access that application and that data. In terms of the local accountability principal, basically what this says is that whenever you make any assertions about authentication or about identity across the network as part of an information exchange, whether you're a sender or a receiver of information, you're going to warrant that those assertions are true and correct.

Over the last two years, we've gathered a number of requirements at a high level with respect to the authentication, and what I've tried to do is list them on this slide and the following slide. We have a basic assertion or a basic assumption that authentication is necessary to facilitate trusted health information exchange. We've kind of taken that as a given, and sometimes it doesn't get articulated clearly up front, so I thought it would be useful to articulate that clearly at this point.

The second point here is that the level of authentication, again, may vary depending on the type of information that's involved in the exchange. Again, this is based on the risk assessment that determines what level of damage would occur should there be a breach with that particular form of information.

The third point is that the participants in health information exchange are authenticated, and these participants may be devices like systems or gateways or services or a process on a machine, or they may actually be people, that is, users of systems. Both of these require some form of authentication when we're engaged in a trusted exchange.

Certain types of exchange may require consumer authentication. I noticed that we had some testimony scheduled from Sean Nolan, I think, from Microsoft, and he has a specific interest in the issue of consumer authentication and how we go about doing that. And so we recognize that as we expand to all of the use cases that are the scope of the NHIN, that consumer authentication is something that we'll need to address in this next year.

Finally, on the last slide here, we believe that in order to insure interoperability of authentication, there must be a standard for communicating the authentication approach. So what our assumption was when we built the authorization framework for the NHIN was applying the local autonomy principal. We would say, okay. It's your decision how you authenticate this individual, but if you're going to make a request of another organization to send a copy of a record, you need to be able to assert certain things about that individual so that the receiving organization has enough information to be able to make a decision about the release of that information based on local policies and preferences that are set within that organization. And so the local accountability and local autonomy of principals when we apply those, it allows us to establish a trust fabric at a technical level where this organization has the autonomy to do what it needs to do to get its work done. It can make the request. This organization has the right to make a decision based on the data that's sent across about the requester and purpose for use and those kinds of things to decide whether to release that information.

I think it's important for us to understand that the model that we had for NHIN node-to-node exchange, and this is not intranodal exchange, which would be local to a particular organization, whether an IDN or an HIE or HSP or whatever they happen to be. Our idea from N node to N node was that these were requests for information, that it's not a remote access in a form of a remote log on to some remote application where you're logging into somebody else's system, but instead these are actual requests for information. There's a decision for the release, and then information is sent across in the form of a recover, in this case, a summary record or whatever type of information that's being requested.

And so, in this scenario that I've just painted, applying the rules and the principals that we've just talked about, we realized early on that we would need to have some framework, some standard for being able to package up data about the requester so that the receiver could make decisions about that. I think it's important that we have, as we move forward, whatever that standard ends up being as far as a recommendation from this committee, that we have some standard for that metadata that's associated with those requests. What we've implemented to date is we are using SAML as a way to do that, and there are authorization authentication and authorization decision components to that, and I won't go into all the boring details of what's in those, but if you're interested, we can have a sidebar conversation about it later.

Otherwise, I think that that pretty well summarizes the general context of what we've got for the NHIN. I think you've already heard that some of these things that I've just articulated, we are going to hear probably multiple times today.

David Lansky – Pacific Business Group on Health – President & CEO
David, could I just ask kind of a clarifying question for me? As you heard the last conversation, both Jim and Wes' questions, and your description of the NHIN thinking, it seems to me there's an awful lot of reliance on the intermediary layer to be the vetter of the authentication activity within that, in this case, NHIN node. And I think you're hearing a little bit of unease, as Wes characterized it, that the competencies of the intermediate layers, as poorly developed as they seem to be in many settings, you know, we have pause over how best to implement the authentication approach that acknowledges those limitations that are out there. How, in the NHIN discussions you've been part of, how are you thinking about the level of competence and the fact that those intermediate layers have to have?

David Riley – ONC – CONNECT Initiative Lead
Well, we didn't necessarily assume that there had to be an intermediate layer. An N node could be defined as an application that's sitting on an end user device that implements the NIN services in order to participate in the larger exchanges. So in that instance, it would be an actual application that's running on an end user device that meets the requirements from a services implementation perspective, and that would be incumbent on whoever built that application to go through that process of implementing the service specs and making sure, through conformance testing, that they actually meet those requirements.

It also predicates. I guess there is a requirement that if you're using some form of third party identity management to issue the credential, that you would be able to get that credential issued from someone else, and then enter that into your application so that that credential is available as a part of the transactions that would be engaged in for NHIN level transactions. But our assumption was not that there had to be an intermediary. We worked with a lot of intermediaries to begin with to understand that. But overall, we realized that there may be instances where people would just simply have applications that would participate in those kinds of exchanges.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks. Any other quick questions to follow-up? Christine?

Christine Bechtel - National Partnership for Women & Families – VP
First of all, David, thank you because that was helpful. I'm not sure that I agree with something you said, and so I want to make sure I understood it and ask you to talk a little bit more about it. And that is that the authentication level is a local decision. And I'm thinking in particular about how do you facilitate interoperability if somebody, if a physician wants to do a particular application or function on the network that an HIE in Dubuque has said that's a level two thing, but where they want to query, they've said that's a level four thing. How do you facilitate that, number one? And then, number two, does it raise a series of trust issues?

I'm thinking from the consumer perspective that if my local HIE has a lot of problems because they really erred on the side of trying to facilitate maximum participation in data exchange by having pretty low levels of authentication, but now that's creating a lot of security risks. But if I just move next door or 100 miles away, it's different. So I'm not sure that I agree with that, but I want to make sure I understood what you….

David Riley – ONC – CONNECT Initiative Lead
Yes. What we were … was that the local autonomy and local – basically the organization, wherever it happens to be, you've got local law. You exist in a state. You may have organizational policies that you have to adhere to. There may be even preferences that are set by providers or patients with respect to the release of information. Those are all things that are going to occur within that organization.
And so, if that organization, let's say they settle on an authentication level two, and they've assessed and decided that that risk is acceptable for those kinds of things that would be involved for EHR or whatever it happens to be, and they're going to make a request to somebody else. What we've said is we have a standard framework for expressing what your level of authentication is, so that's one of the things that goes into the SAML assertion. I'm authenticated at level two. This is the role. This is the purpose for use. This is my user ID, session ID, some of these other things.

Once it comes over here, this organization is not obligated under the law to honor that request. So if I have local policies that say that I require level three, and this guy is asking you. He's coming from a level two. It's my decision over here whether to release it to that or not.

Christine Bechtel - National Partnership for Women & Families – VP
I understood what you said, so that's good and helpful. I think what I'm saying is why wouldn't we or should we think about, and I think it is worthy of some discussion, whether or not there should be sort of a floor set by the governing entity by the nationwide health information network that would say this application is at least a level two, and if you want to make it more or less – if you want to make it more, maybe you can, but you can't make it less. I mean, should that be really a function for the governance of the nationwide network rather than always being a local decision?

David Riley – ONC – CONNECT Initiative Lead
I think that was part of what Farzad was picking at a few minutes ago when he was trying to get the guys that were here to commit to a specific level. In terms of in the workgroup when we were working on the NIN standards, our assumption was that for NHIN node to NHIN node transactions, that it would be a

level three requirement for authentication at the machine level, you know, machine-to-machine. So we wanted strong, a fairly strong authentication mechanism for mutual authentication between the gateways, if you will.

Now in user authentication is a whole different thing that we're working on in terms of how you would transmit. Let's say I wanted to encrypt a package, and I want to ensure encryption end-to-end. How do I introduce that into the existing trust fabric, and how do I route that and do all those kinds of things? Those are active things that we're working on in the spec … right now, working to come up with models as to how we would implement that and support that. But our assumption was that most of the healthcare apps that we looked at would be either level two or level three.

You already have a floor in the form of HIPAA. The Feds have a floor in the forms of FISMA and the requirements that they talked about here. So you already have some disparities between the different organizations that are out there with respect to the processes that have to be in place to insure assurance in terms of the management of information. So the question of whether the NIN governance needs to set a particular standard, I think it's something this committee should wrestle with and make a recommendation on.

I can tell you that based on our experience to date, we think it will be either level two or level three. Most people want to bring it to a level three, and in some instances, if you're wanting to prescribe narcotics over the network, some people have said we need a level four, and so that's a debate that's still ongoing, and I'm not sure will be settled any time soon. But certainly, I think, it's in the purview of this group to make a recommendation about that to NIN governance.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks. Thanks for the question, Christine. Carol has a short clarifying question, and then Wes, and we have to move on quickly.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
A very short clarifying question: When you say there's a standard for communicating the authentication approach, is that from a third party's assertion, or is that just one party saying to the other, this is what I'm using? I worry about the verifiability of that.

David Riley – ONC – CONNECT Initiative Lead
What I was speaking at here was the standard for the envelop that you packaged around your message that says, hey, I would like to know if you have this patient. And, if you do, I would like this record on them. The metadata that's in that header about the requestor and purpose for use and all of that, we've been using the SAML standard in the NHIN for that for expressing that, and we have the authorization framework service specification is where all of that's detailed. It has authentication authorization, authorization decision components to that, if you're familiar with SAML.

And so, basically, what's going on inside the organization at the EHR level, we've been largely unconcerned with until they get ready to make a request outside of the organization. And then, at that point, they need to be able to populate the SAML assertion in order for the receiving organization to be able to process that in a computable fashion and make a decision about the release of that information. Does that answer your question?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes.

David Lansky – Pacific Business Group on Health – President & CEO
Wes?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I just want to make sure I've got applicability straight here. At one point, I think I understood, and I think it's still true that the work that's been done in the NHIN is towards interconnecting HIEs and other organizations that, for some reason, wouldn't want to put an intermediary between them and the other organizations.

For various kinds of computer-to-computer transactions, and it almost sounded like any means of identity, then any use of identity of a person in that environment is almost for the audit trail. It says, yes, we can tell you who, back in the real world of people users, initiated this inquiry or something like that, but it's not for the other side of the connection to grant access to an application directly. It's computer-to-computer.

David Riley – ONC – CONNECT Initiative Lead
Yes. Let me clarify that because we're not saying, at least in the way we modeled the NIN transactions, there was not a remote access to an application. It's a request for a record or a summary record to be sent. We're not talking about remote log on or remote access to anything. It's not, you know, you're not looking in somebody's inbox over here. That's not the kind of transaction that we've modeled, and so the release of information, right now what we've implemented, at least in our CONNECT solution of the gateway, there is a policy engine that takes that SAML assertion and local XACML policy documents, and actually processes those and makes a decision about the release of information, whether it's released or not. And so the SAML assertion plays a role in that. If I have a policy that says I won't release to anybody that authenticates at level two and, in your assertion, you assert a level two authentication, then as a part of that processing of the SAML and the XACML policy that I've got locally, it would make a decision not to release that information.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I know David wants to move on.

David Lansky – Pacific Business Group on Health – President & CEO
We need to move on.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I'll ask the question offline….

David Riley – ONC – CONNECT Initiative Lead
The other thing I would point out, Wes, you were out of the room when we were talking about whether it was organization intermediaries. We've not made assumptions that it would be intermediary based. We've assumed that a NIN node could be an application sitting on a computer just so long as it implements those interfaces.

David Lansky – Pacific Business Group on Health – President & CEO
Good. Thanks very much, David, for coming.

David Riley – ONC – CONNECT Initiative Lead
You're welcome. Thanks.

David Lansky – Pacific Business Group on Health – President & CEO

Let me bring up the next panel of VeriSign, Covinsint, Anakam, and Bio Pharma, and again, thank you all for coming today and helping us sort through all this material. Given that we're a few minutes behind, I'd very much appreciate it if you could really confine your verbal comments just to a few key points, so we can have the conversation continue with all of you. With that, let me start with VeriSign. Nick, could you just introduce yourself and jump right in?

Nick Piazzola – VeriSign – VP Federal Markets

Good morning. I'm Nick Piazzola, the vice president of government programs at VeriSign, and I thank you for the opportunity to speak today. In terms of my own background, I have some 41 years of experience in information security, 28 at the National Security Agency and 13 at VeriSign, so in all those systems, I have had extensive experience in design, develop, and deployment of systems. I have some practice insights into what it really takes to deploy large-scale authentication systems.

Let me begin by just making a few comments about VeriSign, and I can summarize the key points about your questions, and I have some specific recommendations for this committee. In terms of VeriSign, we're a provider of infrastructure and trust services for the Internet. For those infrastructure services, we provide the authoritative directory of some 93 million dot-com and dot-net Web names. We also operate the root server for the domain name system that enables the look up of domain names and associated IP addresses. We process some 50 billion of these look ups called DNS queries every day.

More importantly, we also provide identity and authentication services that enable trust for users, devices and Web sites on the Internet. The fundamental problem that we're trying to solve is enabling trust by providing the capability to identify and authenticate, that is, validate the identity of entities participating in transactions on the Internet. Our primary offerings that enable trust in Internet transactions are digital certificates issued from a VeriSign managed public key infrastructure for both individuals and Web servers, and one-time password devices to enable strong, although known as two-factor authentication, primarily for remote access to Web sites.

Our users can be grouped into three categories: organizations with a Web site on the Internet; affiliated individuals, employees of a corporation or a government agency; and consumers. In terms of our customer base, our SSL digital certificates provide identity and protection for over one million Web servers. These include most of the Fortune 500 companies, the world's largest banks, top Internet retailers, and 3,000 healthcare companies. Related to healthcare use of digital certificates, we recently partnered with CAQH to pilot the use of VeriSign certificates to protect the exchange of health information between payers and providers.

The VeriSign secure site seal, which is displayed as a sign of trust on VeriSign protected Web sites, is viewed over 175 million times a day. We operate more than 1,000 managed PKIs for government and commercial customers that range in size from less than 100 users to more than 600,000 users. And we've issued over 2.6 million VeriSign identity protection credentials to consumers for one-time password based strong authentication at network leading Web sites.

On the question of who pays for these solutions, there are two answers. For digital certificates issued from a managed PKI operated on behalf of a government agency or commercial business. The customer pays all the costs and, additionally, provides the personnel to perform the identity proofing of the employees or other affiliates of the organization. For the issuance of digital certificates to Web sites and unaffiliated individuals, VeriSign provides all of the required implementation operation support costs, and these costs are amortized across the entire base and user that's reflected in the price of the certificate that the user pays. For OTP solutions, consumers can buy an OTP device in VeriSign or more than a dozen other vendors or, if they have a Blackberry, iPhone, or other smart phone, VeriSign provides a free download of an OTP software to these devices, and the corresponding validation services for OTP are paid by relying parties.

One of the primary issues with respect to the cost and widespread deployment of identity authentication solutions is who will provide the identity proofing of users, which is particularly challenging if you have a large number of widely disbursed users. This issue requires either the delegation of identity proofing to trusted agents or the use of alternative methods such as online knowledge based authentication. All of VeriSign's authentication solutions support a delegated identity-proofing model. My sense is that some combination of delegated identity proofing and knowledge based authentication will be required for the NIN.

On the question of directory services, I wasn't quite sure the thrust of your question, so let me just say that we understand the need for directories, and VeriSign providers very large-scale directories to support both our DNS and PKI services.

Finally, in my opinion, the most important near term issue that the committee should consider is the question of what is the minimum assurance level for identity proofing of individuals who have access to personal health data on the NIN. You may decide or probably will decide there are different assurance levels for different categories of users. Some may require personal presence of identity proofing. For others, knowledge based authentication may be acceptable. You may decide to characterize your assurance levels in the context of 800-63 defined assurance levels. But as some indicated, you may find that too restrictive or may be difficult on a very large scale to deploy if you do precisely what 800-63 requires.

I would also encourage you to look at OMB policy M06-16. It relates to protecting access to personally identifiable information. It provides sound guidance, which states that access to PII should be done with two-factor authentication where one of the factors is the device, which is separate from the computer being used to gain access. My concern is that a NIN that only requires user name and password for access to personal health information will inevitably result in significant exposure of that data. Once you've established the policies related to these core issues of identity proofing and two-factor authentication, I believe you will find there are many vendors who can provide competitive identity authentication solutions for the NIN. Then the other important questions of federation of different credential types and who will provide compliance assessment can then be addressed.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you very much. Mr. Miller?

David Miller – Covisint – Chief Security Officer
My name is David Miller. I work for Covisint. Just for those of you who don't know who Covisint is, Covisint basically provides an interoperability platform. The way we look at it is kind of enabling the information ecosystems, and that's what healthcare is coming to is this idea of an ecosystem. I'm very interested in the fact that you guys have decided to tackle this idea of authorization because, for security people, authorization of users is almost a religion. Some people love certificates. Some people love one-time passwords.
It becomes very difficult, and so the points, and you've got my testimony. You can kind of read through some of it, but the things that I really thought were important is the first thing is to really understand that there are two aspects to authorization. The credential, the thing that is issued to me, the certificate that I use, the one-time password that I use, all that does is that authenticates that I'm the person who got the credential. It doesn't say I'm Dave Miller. It just says I'm the person who was issued the credential. And

there are lots at this table. There are lots of vendors who provide technology services that do that in a way that is probably fairly unhackable.

The second aspect, which you did bring up, which is the administration, is how do I know that Dave Miller is Dave Miller? How do I get him a credential? How do I get the credential that says he's Dave Miller appropriately? That actually is an extremely difficult process. That's where the hard part is. You could decide that you're going to use a PKI solution, and I can tell you. Those are DoD level type, you know, you're not going to hack that. But how do I get that to the person? That is a difficult model.

In most cases, what we've seen at Covisint is this ability through the idea of making identities interoperable is push it off as far, as close to the organization that owns the end user. Now that doesn't work all the time. We certainly do have physicians that sit in small offices where they don't have an organization that owns them. But for a lot of physicians, they have hospital systems. They have other things, and they have the ability to manage the issuance of a credential, and so that's the first thing is that ability to do that, and then be able to reuse that credential.

But the thing that I think is most important about this authorization is the fact that the end points in these cases are people, not systems. And people believe that they are the most secure thing in the world, and it's the rest of the people who are insecure, but they are very secure. So I shouldn't have to be required to do something like have a certificate or a card. I'm very happy for everyone else to have one because they're all insecure, but I'm perfectly secure enough to have a password. And so when you have that, the issue becomes that you can come up with this wonderful policy that says you're going to do level three, and level three requires the issuance of something that is physical, and you can even force that, and users will find ways to get around that security if they don't believe that they need to follow that level.

In a previous life where I was issuing those wonderful little tokens where the numbers change all the time, to a group of executives, one of them had his kid set up a Web can, and he put the token in front of it and then he would go onto an unsecure site, and he thought it was the best thing ever in the whole entire world. So those sorts of things, you have to be able to keep in mind is the issue that says I can come up with a policy, and if that policy is something that, in the end, a physician is not going to use, then they will find the most unbelievably insecure way around it. That executive would have been better off having a password than what he did. What he did was much less secure than a password, even though the technology was an unbelievably secure technology. So that is an unbelievably important thing to be able to determine.

The last thing is the fact that one of the ways to really solve now, maybe not solve the problem, but one of the ways to be able to deal with the problem is to reduce the number of authentications a user has to do. In these discussions about authentications, I'm used to working in an enterprise where we're trying to figure out, for the enterprise, what is the one credential that everyone is going to use. For example, HSPD-12 is for the government. The government is an enterprise. I'm going to issue one credential. You get your HSPD-12 credential, and hopefully that's used everywhere.

This isn't the way this is working here. We're talking about physicians accessing data that sits at multiple external places, so let's say that you come up with a great solution for authentication. But as a physician, for me to get information on a patient, I have to enter that 20 times. Again, I may like it for once, but I'm not using it 20 times. A real good example, a real world example of this today is the current rules that the DEA has for the e-prescribing of controlled substances. So they want some sort of physical token. That's all right. And they expect the physician to reenter that token code for each prescription.

If I’m going to prescribe you three controlled substances, I enter the number three times. That’s enough for physicians to find ways to go … right? That’s enough for them to figure out some way. You know, I’m going to put it in front of a camera that does character recognition, and then it’ll enter it for me, and then I don’t have to worry about it. In that area, if there was a way to be able to say, allow a physician to be able to authenticate locally, and then be able to use that authentication in every place that they go, you can then make that local authentication a better local authentication.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks. Very helpful. Mr. Williams?

Brent Williams – Anakam, Inc. – Chief Technology Officer
Good morning. My name is Brent Williams. I’m the CTO of Anakam. We’re a little different than the other vendors that you might be talking to. We sell software. We actually are purchased, much like the government agencies. The organizations that are represented here actually install our software, and the enterprise run it. Some of these organizations at the table actually use that software to do that.

We do two-factor authentication for extremely large-scale audiences in the order of millions of users, and we also integrate that fully with level three, level two, and level one identity proofing remotely, as well as professional credential verification, so we can actually figure out are you really the carbon based life form of Bill…. Are you actually a board certified physician? And then issue you two-factor authentication credentials for those.

We have 11 federal agencies as clients right now. Half of our business is in the commercial healthcare marketplace, and what I want to do is share a lot of that experience base specifically from interacting with the HIEs and the RHIOs that have deployed our product and are actually using it now across both the patient and the practitioner side of the interaction.

First of all, this separation between authentication and identity proofing. I can’t emphasize to you what Dr. Alterman said to you earlier today is that needing to be able to separate identity proofing and authentication and then the other downstream processes, and understanding that each of those has a different set of standards associated with it. One of the things that we’ve learned in this process, and I’ll use a PHR as a great example. A self-subscribed PHR that a patient is putting the information in, the patient will still want to protect the information with level three authentication, but level three identity proofing is not necessarily required. I’m putting my own information in there. I just want to secure it. I don’t need to prove that I’m who I am to myself. Remember that when you say level three, differentiating level three authentication from level three identity proofing is critical.

Now, at the same time, David Temoshok back there is probably going to turn around and say, and Tim Polk, are both going to say what’s important about 800-63 is understanding that the total level of the credential that’s issued is a function of each of the pieces. Level three identity proofing, plus level three authentication creates a level three credential, and that’s important too. But understanding that there are business processes within the healthcare industry where we want to separate out those requirements and give the fine grain requirement to them that you don’t necessarily need level three controls on either are as important.

Secondly is the concept of federation. Federation has been lost in this, frankly, and I’m going to give a fairly unvarnished view of this. The reason federation was invented and exists is for the basic concept that I am running an organization, and I want to bring in people from another organization, and I’m going to trust them because I trust the way this organization has them. So organization A has Brent Williams enrolled. Organization B does not have Brent Williams enrolled. Organization B might have Brent

Williams' medical records, but he's not enrolled to have access to the system. He doesn't actually have a name in the directory.

So then, organization A conducts the authentication. You click on a resource that says I'm going to go to organization B, and organization B says what's the assertion of who this is that's coming in? And if you say it's Brent Williams, I trust it. As soon as Brent Williams appears in that directory, and you give Brent Williams privileges in organization B's directory, and you have to enroll Brent Williams in that system, federation is lost. So understand the purpose behind federation. It's accepting an unknown individual into an organization because somebody else trusts them.

As soon as you start telling those people they've got to enroll in your system because you're going to give them special accesses and privileges, it's no longer federation. It becomes a fancy way of doing single sign on, so let's all get that out on the table because what you may do is you may be able to find more cost effective and more efficient ways to be able to do the implementations.

Now the other part of this discussion was brought up by the government representatives up here earlier, and I can't overemphasize it. The number of places that I've walked into, whether it's the federal government or state and local entities that have deployed our software that have purposefully said this is level two information because I can't afford to deploy a level three solution. It's why we invented our software. Level three is perfectly cost effective to deploy at a very cost effective measure for millions of users. We have sold the software to the government. We have the largest level three citizen facing solution in the federal government right now, hundreds of thousands of users. The point is that it's doable. Don't let people dumb down the information or even just call it level two when it's not actually level two.

The other point is that the standards do exist. Now one misnomer out there is people throw around HIPAA, FISMA, the Privacy Act as requirements. Unfortunately, none of them actually set thresholds. They all say risk based. So when you're actually talking about thresholds, and that's what you all want to get to today, is the fact that the thresholds do exist, but when you cite the thresholds, you're going to be citing OMB M06-17 or M06-0717, M04-04, NIST level three through special publication 800-63, so make sure that the citations that actually call out what levels you're going to reference documents that are specifying what they are. For example, when working actively with states of California, Texas, Florida, and they say there's not a HIPAA requirement that I have to put in level three, well, do you want to do business with the federal government, because this document then does it, and so you have to weave that federal requirement on how to get there.

Lastly, there are numerous proposals that are in front of the Office of the National Coordinator for what we call the National Electronic Healthcare Identity Capability. Notice I didn't say credential. NEHIC, and it's the concept of being able to put within a context how HIEs, RHIOs, large enterprises, practitioners, equipment resellers, everybody who plays a role in the healthcare enterprise understands where an identity presents itself in the enterprise, whether a practitioner is coming in through a hospital organization, whether a practitioner is presenting themselves through their own practice, or whether they're just logging in from home and coming in through a portal, how they authenticate in that environment and how their identity is trusted.

Critical to this is understanding the role of the patient and the fact is that when a patient logs in to Dr. Smith's healthcare record system and says, I want to see all of my records, and being able to find that patient in a larger system in the NHIN is going to be challenging, and so being able to get the level of authentication up. The NHIC paper defines that, and I'm more than willing to provide it otherwise. So the example use cases, what we say is that it's not based upon the applications. I've heard that word come out a couple of times today that we have to set the level based upon applications.

It's actually better to say that it's based upon business use case. And so the business use cases that we've isolated are patient access to their own medical records, patient access to family members' medical records, practitioner access to multiple patient records, administrator access to multiple patient records, and administrative access to system controls and activities. So understanding each of those has level three requirements for authentication and level three requirements for identity proofing.

The last thing I'll say is that this is probably going to be heresy in this room is that one of the things that we've learned when we get down to assertion technology is people call PKI authentication. Unfortunately, PKI isn't authentication. PKI is a way for machines to authenticate to each other, so what Dave said is really important. It's all about the carbon based life form that's sitting on the other end of that computer, and it's not about who's that computer authenticating to the system. So certificates and PKI do a great job of being able to communicate who is sitting at that computer. But in the end, the authentication processes that release that certificate, the authentication processes whether they're machine based, whether they're a token or a device based, or whether they're cloud based that let that PKI fly just like it's a SAML assertion. So understand that in the context that we've seen it, it's better to think of PKI as an assertion technology like SAML is an assertion technology when you're trying to drive those standards. I'll leave it at that.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks very much. Mollie?

Mollie Shields-Uehling – SAFE-BioPharma – President & CEO
I'm Mollie Shields-Uehling. I'm CEO of SAFE-BioPharma Association, and on behalf of our community, I thank you for inviting us to testify today. SAFE-BioPharma Association is different, I think, than my colleagues here on this panel. We are a nonprofit collaboration that was established by the world leading biopharmaceutical companies to establish a digital identity and signature standard for the industry, a standard that would allow the industry to really transform its business processes to fully electronic.

Today the standard is – we were created in mid 2005. Today the standard is recognized by the FDA, the European Medicines Agency, we meet HIPAA and EU data privacy requirements. Our system and standard is interoperable with the U.S. government identity management system. It is vendor and technology neutral, and it comprises a system of governance and operating policies to which every member, issuer, and participant is bound by contract.

With that, I'm going to sort of very briefly summarize our responses to each question. Regarding trust, the SAFE standard was developed to provide really the sector with high trust that who you're dealing with on the Internet is who he or she says he is, and that that identity is uniquely linked to a digital signature. Secondly, our credentials are currently held by biopharmaceutical company employees, by contract research organizations, by clinical investigators and their staff, by healthcare suppliers, by physicians, by outsource IT providers, by contractors, regulators, and others.

Because there are a number of cross-certified issuers, we do not maintain a directory of the total universe of holders. However, between the growing, very substantially growing SAFE-BioPharma Association community, certainly CertiPath, the U.S. government holders, and sort of the growing network of cyber communities, there are millions and millions of credential holders that are interoperable credentialed.

Who pays for the solution? First, I think the SAFE standard accommodates multiple levels of assurance and token form factors. We provide for identity proofing through an online antecedent process, which takes about 15 minutes from start to completion, and can check medical license information. It can be done by notary, and a notary will go to the home or office of a doctor, physician, or other user to do these face-to-face, or by a trained, trusted agent.

The costs really vary depending on the size of the implementation, the type of identity proofing, the form factor, etc. However, that said, the costs are coming down very, very substantial. They have come down over the last number of years, and they continue to decline, as these deployments increase.

We believe that all of the essentials are in place, the fundamentals for widespread deployment. There are interoperable standards available. There are technologies. There are processes. There are providers, and there's a growing network of users. What we believe is needed is certainty and guidance regarding what is an interoperable, digital identity standard and how it will be applied to the NHIN.

Directory services, first, the SAFE-BioPharma standard and credentials fully align with federal PKI authority, and we are cross-certified with the federal bridge. All of the cross-certified issuers are also cross-certified with the federal bridge. We believe, similar to our colleagues here, that authentication and authorization are separate and distinct phases of the process of gaining access to information. Multiple sources can provide credentials. However, the owner of the information or the manager of the information should manage the authorization phase. We support the role of emerging identity service providers in a federated identity, and we are working with the U.S. and European governments, as well as leading standards organizations to maintain alignment.

Regarding a delegated authentication model, we support delegated authentication in three ways: first, through cross-certified issuers; secondly, a number of our member companies have built enterprise-wide infrastructures and cross-certified them with SAFE; and third, the SAFE-BioPharma Association maintains a registration authority for use by our members and their external partners.

What should be, I think, probably the very important question today is what should be the role of government. We believe, it is our position that the U.S. government has a well-developed and broadly accepted set of interoperable identity management standards and processes. These are managed under the purview of the Federal CIO Council, and certainly incorporate ICAM and the Federal PKI PA, which you heard about earlier in an earlier panel.

This trust system is used by millions of government workers and contractors. It is supported by an expanding number of commercial providers, and it is a common platform for a growing number of cyber communities, including the SAFE-BioPharma community, the CertiPath community, and potentially a number of others. This trust system meets the NHIN's privacy, security, and confidentiality requirements. Most importantly, it is scaleable. And we recommend that the U.S. government extend these interoperable standards and processes into the NHIN. And we believe that the affect of this extension will be to provide a certainty around the operating environment to spur the growth and evolution of the NHIN and the use of sensitive healthcare information and certainly will support the goals of meaningful use. Thank you.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you. Thank you all very much. Very provocative testimony for us. Let me see who may have questions. We'll start with Micky and then Farzad and go around.

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO

Thanks to everyone. Just building on something that Dave Miller and Brent Williams were talking about when you sort of think about, you've got to have the individual users care enough about the issues that we're talking about and get the convenience level down to a point that they're willing to actually use whatever systems we have in place, and the need for something physical. Could you elaborate a little bit on cell phones as perhaps being, you know, that's something physical going forward? I think, you know, Nick Piazzola, and I hope I didn't butcher your name, you talked about the NCP at VeriSign, but I'd love to know more about what the state of that technology is and whether you see that as being something going forward because having individual physicians, whether it's in Spearfish or Lowell, Mass, really robustly use tokens, just some kind of key fob thing or something like that just feels like it's going to present a huge adoption issue.

Brent Williams – Anakam, Inc. – Chief Technology Officer
…start with that because our fundamental operation is based on tokens, and what I would say – or based on cell phones – is operating as a token. What I would say is you brought practitioners into this space, and what we've learned very rapidly in this marketplace is that while we'd absolutely love for practitioners to adopt cell phones as being fantastic devices to use inside the enterprise, what we're learning is this concept that there has to be a blended solution. There's not one size fits all for everybody, and so that the doctor's ability to walk up to a workstation or a nurse's ability to walk up to a workstation and have some procs badge cause the workstation to recognize who they are within the facility or a physical ID card, to have the physical ID, much like the HSPD-12 principals in the federal government are absolutely critical. So it's understanding the role of a cell phone in that transaction is that the cell phone could be used, and we'd love it if everybody bought them, but we recognize we've got to fit into more of an ecosphere of authentication solutions, and that the cell phone is really better for people who are going to be going to a lot of different enterprises and not wanting to carry around 14 different cards or tokens hanging around their neck, and going to be authenticating remotely to those systems, and potentially infrequently to those systems. So it's a function of convenience.

Now the other thing that you should know about using cell phones is there are lots of different ways to use a cell phone to authenticate. You could download software and put it on the cell phone and then it generates codes, and it looks like those tokens people carry around their necks. There are ways to actually – our technology is to send an SMS to the cell phone, so you don't have to put any software on the phone. You can also call the phone, and actually deliver it via voice. So the key is being able to meet with the ADA and Section 508 requirements, and being able to interoperate with as many different people, the ability to leverage telephony, not just cell phones, but all forms of telephony, so cell phones don't work in cath labs underground. Pagers that work in hospitals, being able to leverage them as part of your infrastructure, and understanding how they play together, we found is critical to that, so knowing where it fits and who is going to use it. It's still level three technology if it's implemented properly, but understanding how it fits in that total ecosphere is critical.

David Lansky – Pacific Business Group on Health – President & CEO
Dave or Nick?

Nick Piazzola – VeriSign – VP Federal Markets
Yes. The only thing that I would just add to that really kind of highlights that Brent brought up is the fact that it's not a single. Users shouldn't be issued a single credential. A user may have three credentials depending upon the locale, for example, that they access. The way the real world works is that after I authenticate myself into a building, for example, I have some access that doesn't require me to authenticate again by virtue of the fact that I'm in the building. For example, a doctor in the ER is in the ER, and he's in the room. He may not have to use a second factor authentication because the second factor is kind of the fact that he has a badge and he's there, and he's in front of a bunch of people who

recognize him. As opposed to the person who is accessing from their – a doctor who gets called in the middle of the night and accesses on the Internet where it's like, okay. Now I want a second factor. So a single solution just won't work. You either will create a single solution that is not secure enough for remote type access, or you will create a single solution that is a total pain if you're local.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks, Nick. Any other comments?

M
I would just say that in VeriSign's strategy, the use of the cell phone is critical for widespread deployment to consumers. And there's some 90 million that have cell phones today. The idea that they could – don't have to pay for a separate token, can use their existing cell phone either in our concept, download software to that device and be able to just read off the code from the device, or get an SMS message are practical ways to get two-factor authentication to consumers at very low cost.

David Lansky – Pacific Business Group on Health – President & CEO
Farzad? Mollie, you have a comment.

Mollie Shields-Uehling – SAFE-BioPharma – President & CEO
When SAFE started out, we were sort of a one size fits all standard. And what we found, we credentialed a whole bunch of doctors, and what we found is that just doesn't work. You need lots of different options for different settings, and so I would agree with everything my colleagues are saying here.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks. Farzad?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Back to the last time when I thought we were done, and now you guys introduced the identity proofing versus authentication wrinkle, and I just want to ask you. Are there, among that list the government maintains of organizations, many of them you're included in that, who can provide a certain level of assurance in terms of the authentication, does anyone provide also level three identity proofing that is commercially available, that that doc in Spearfish can access?

M
On the current list, they do level three face-to-face. Level three remote is not available on the current list. However, level three remote is available commercially unlisted.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
So there are current providers of credentials who will do face-to-face identity proofing. I didn't hear whether it's affordable or not and scaleable to Spearfish, Montana. But you're saying while there are commercially available, remote, and again, this is knowledge based.

M
Knowledge based, yes.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Knowledge based identity proofing that those have not yet been recognized by the federal government as meeting.

M
To be honest, there's – I've got to differ a little bit with the government panel that was up here a little earlier because the mechanism for getting recognized, the mechanism is not as well defined. There's not a certification path for, say, a software company to get certified as being level three. It's a self-certifying process if you meet the standards.

The certifying, there are providers, credential providers that provide the end-to-end, much like SAFE-BioPharma does or something along those lines, that they are certified for providing credentials at a certain level, and they have a mechanism, and that process is audited and supervised and monitored. That's done through a procurement process, and an audit and oversight process. Whereas, there are any number of vendors in the marketplace today that actually do remote antecedent data, identity proofing that would meet the government identity-proofing requirement, and that process for doing that is not certifiable in and of itself. It's the whole process that's certifiable. It's much like certification and accreditation. You can't certify and accredit a piece of a system. You've got to certify and accredit the whole system.

Mollie Shields-Uehling – SAFE-BioPharma – President & CEO
I'm not sure that we're talking about the same things, but in terms of providing a physician in Spearhead, Montana a credential, and do to the identity proofing, that process exists today, and it is incorporated into the federal government rules and regulations. It is available to SAFE-BioPharma members. And so, for example, as I mentioned earlier, a doctor can log on, complete an identity proofing process, which relies on an antecedent face-to-face, and which….

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Sorry, which does or does not rely on?

Mollie Shields-Uehling – SAFE-BioPharma – President & CEO
I'm sorry.
Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
It does rely on the face-to-face.

Mollie Shields-Uehling – SAFE-BioPharma – President & CEO
Yes, relies on an antecedent face-to-face, and it takes disparate databases, and it has a knowledge based process in which the identity is confirmed, and then the doctor actually or the person signs an end user agreement, downloads, if a downloaded certificate is required, and is enabled. So the identity proofing and the credential disbursement really takes about 15 or 20 minutes, so it is available today. Yes.

David Lansky – Pacific Business Group on Health – President & CEO
The antecedent face-to-face piece again, that seems critical, and I don't think we understand it.

Mollie Shields-Uehling – SAFE-BioPharma – President & CEO
Okay. So there are many processes that people go through to have a face-to-face. For example, most states in the country require a face-to-face for doctors' licensing. A face-to-face is required for bank accounts. It is required for a number of other processes. And the federal rules allow you to rely on one of these earlier face-to-face that you can access through various databases.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you.

M
What I want to clarify is, you asked the question, are they on the list now as certified remote, and the answer is no. Are you standards compliant? Are there standards defined? Absolutely, and there are numerous providers who are compliant with that standard. So what I'm trying to caution the working group is if you say only use the three providers on the GSA list, you're going to leave off a multitude of providers in the marketplace who are capable of meeting the federal standard, yet and could drive the cost and the adoptability down if you say it's only that list of the GSA accept….

M
I would direct a little bit of that question maybe back to NIST because I think NIST has some problems with being able to quantify the performance of a knowledge based authentication system. I think they're practical and viable, but they're not all the same. It's a function of the quality of the data in the database, the number of questions that get answered, and all that. So I think part of the reason you don't have a list of approved identity proofers using knowledge based authentication is they don't know how to write a standard for that or a set of criteria for that. I'm speaking on behalf of NIST. You should direct that question to them.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks.

M
The other thing, and this is just if you look at level three, and I'm going to kind of just go back to the issues that have come up with the whole DEA, e-prescribing of controlled substances. They were looking for level three accreditation physicians, and the idea was level three requires face-to-face. And the face-to-face would be at hospitals that provide Medicare capability, and the physician said, I don't want to have to go to a hospital. I'm an independent physician because I don't want to be associated to a hospital.

The hard thing about face-to-face is the face. Who is it? Is it the federal government? Do I have to go to my post office? Do I have to go to – and so that becomes an extremely difficult issue that has, by the way, nothing to do with security or the ability to do it. We issue passports and drivers' licenses all the time, and that requires face-to-face. That's there. It is the, is government willing to say I'm going to require you, as a physician, to go to a place that I'm going to dictate that is going to vet who you are, and that is some place where I don't believe the U.S. government wants to be right now.

M
The problem is there aren't any places to go, so the only practical way to do face-to-face is that, A, you delegate it to some trusted agent inside an organization, and that agent can then do the face-to-face identity proofing of the people inside the organization. Or you ask those people to go to a notary. Both of those approaches are acceptable to the federal government, and then you get … level three for whatever kind of credential you want to issue.

David Lansky – Pacific Business Group on Health – President & CEO
I want to move on. We have a short time and a couple more questions queued up, so why don't we go to Jim and then Arien and Wes.

Jim Borland – SSA – Special Advisor for Health IT, Office of the Commissioner
I'm just curious. Based on your experience, and I know that some of you were HSPD-12 credential vendors. Obviously with all of the agencies subject to HSPD-12, their credentialing system, their identification systems were rip and replace based on the new requirements. So looking at that situation in

the healthcare market, are we looking at a very, very high percentage of healthcare organizations that in order to meet this kind of a standard, are going to have to rip and replace?

M
Our experience is with identity federation, which is actually fairly, actually fairly mature from a standards standpoint, is 98% of the organizations we talk to say I don't have any tools to be able to accept it. The first issue is how do you issue the credential. Now it's the, what systems can accept it? I mean, the question asked about HSPD-12 is what percentage of federal government IT systems have the ability today to accept an HSPD-12 certificate as authentication, and it's very low because that technology is just not there. Yes, there's a lot of rip and replace.

David Lansky – Pacific Business Group on Health – President & CEO
Arien?

Arien Malec – RelayHealth – VP, Product Management
We talked a little earlier about scaling some of this up from the tens of thousands to the millions in terms of number of providers and staff, and I'm very conscious of this tradeoff that Dave mentioned between usability and security, and then between usability and cost. I want to scale this up two more orders of magnitude because part of our charter is how does that provider then provide the patient's information to the patient. So it's no longer the patients self-managing their own data. Now the provider is sending information to the patient's designated PHR. And although I can barely wrap my mind around providers doing level three identity proofing and level three authentication, I'm having a hard time wrapping my mind around both the identity proofing portion and the authentication portion for patients. I'm wondering if you guys can address that.

M
If we're talking about 100 million or 200 million users, then we're not going to be doing face-to-face identity proofing. It's just not practical to extend it out to that. We don't have enough trusted agents. We don't have enough notaries. There's just not practical way to do that.

The reality is that to get a high level of assurance, practically they're just going to have to use knowledge based authentication. That can be done online. If you go to the full NIST standard, it requires some proof of that process having been done, sent to the user's home address, but there may be some way to work your way into that or maybe accept something less than that. But some practical form of online knowledge based authentication is probably the only way you're ever going to be able to identity proof 100 million, 200 million people.

M
The one thing though that I think is different here is you're talking about healthcare data. And for healthcare data to be generated on me, I have to have seen a physician. Use the physicians. You want to do face-to-face. Let my physician vet me. He vets me all the time anyway. I mean, when I walk into his office, he knows who I am, so leverage that capability. Allow the physician to be able to issue the credential to the patient and manage that, and actually, interestingly enough, maybe be able to see what I'm looking at. Am I a patient who is not looking at his information? In the same way, do I get my prescription filled? You could leverage that.

You could leverage pharmacies. Pharmacies see me, so to get my pill, I have to do face-to-face. I mean, I know that there's certainly the online type of thing. That is a place to leverage.

M
There's a happy medium point in there too that's also usable, and that is leveraging installed infrastructure bases like HIEs and RHIOs because, in all reality, that's a place where they can have the equipment and the infrastructure to manage and operate it because, in Spearfish, Montana, they're not going to have the equipment running in that particular facility. Dr. Alterman really got us going on that one. But, at the same time, the RHIOs and the HIEs that are seeing the information flow between the organizations can then have the system and provide the capability for people to be either remotely identity proofed or have people that are delegates to do face-to-face within that infrastructure, whether they're practitioners or not.

David Lansky – Pacific Business Group on Health – President & CEO
Right. Let's move on to Wes.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I have one, I hope, quick question, and it has to do with the issue of some organization proofs the identity. Some organization relies on that proof in order to authenticate the user. Then some organization conveys that authenticated status and identity of a user to another organization. I didn't mention certificates here, and it's not clear to me where does the certificate – how does it get issued? Where does it get placed? If I go, and I fill out a form, and then a notary comes out and visits me, what happens electronically then going forward, and are the standards in place and in use for that, through that entire series of steps that I…?

M
They talk about this, right? Basically what it says if you do identity-proofing separate from credential issuing, then you have to have a mechanism to bind the identity proofing to the credential. There are a number of ways to do that. I participated recently in an ICAM study that looked at the possibility of using banks to do identity proofing of individuals so that they could then get a credential that could be used to access a government benefit. And the conclusion that came there was there probably needed a piece of infrastructure or a third party entity that actually passed that binding from the identity proofer to the….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
And by a credential, you mean something physical that they can hold, or do you mean…?

M
Well, the credential is whatever form it takes. It could be a piece of software that is a digital certificate. It could be a digital certificate on a hardware token, but whatever it is that identities you is your credential. Then to get that credential, you have to be identity proofed, so the question is how do you link those two together. There are a variety of approaches that do that.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Sorry….

M
We can actually do that in the PKI world, but basically it involves – the user has to come to the system first and enter some data and get some information. Then he takes that to the notary, for example, and then when he comes back, we're able to link him back up or bind that information that we gave him the first time so that we know that the person that got the identity proofing is the person who is coming back to the get the credential.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So….

M
…technical challenge … bind them together.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
…that we know how to get proof and identity, and bind it to something. Bind it to what? Bind it to a digital certificate, purely, bind it to a device? I mean, I'm just – how this gets conveyed through the IT system is what I don't understand.

M
The digital certificate actually is a full credential in the sense that it carries your identity, so your identity gets embedded into the digital certificate.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
But it's not a … it's bits someplace?

M
It is bits. It is absolutely bits, but inside that, there's a format for that, and inside that, that's….

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I understand that.

M
And so you have to protect that on your workstation. If you want it to be portable, then you have to put it on a token to be able to take it with you.

M
One way to do this, so you can do it the way that they did it in Canada. Canada said we're standardizing on certificates. Here's the container in which that certificate is going to be in. You're going to go to a government office. They're going to look at your face and look at your drivers' license and look at other things, and they're going to hand you a physical thing that is yours. And, oh, by the way, the other thing the Canadian government said is if you misuse this, we're going to put you in jail. That's what stops people from misusing it.

But if you don't want to do that, you could have it so that I go to the identity store, and there are 20 possible things. I can register my phone with Anakam. I can get a certificate on a smart card. It's whatever thing I want, and they have that ability. But in the end, I have to walk away with a thing because it's the security weakest link is if you separate the issuing of the credential from the vetting of the user. Then that's where I hack.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
And that thing has to be able to convey the bits that are the digital certificate to some other thing. Is that right?

M
Yes.

Brent Williams – Anakam, Inc. – Chief Technology Officer
Wes, go back to my heresy in there where I said PKI is an authentication. It's an assertion technology because what you're talking about here is you get a string of numbers, and that's what PKI is. It's a string of numbers. So the key is then there's an authentication rule set that's established about how that string of numbers is allowed to go flying away from whatever you stored it in, and go to somebody else's system and say it's you, and that is at a level three thing that allows it to go flying. Is it a level two thing that allows it to go flying? And where is it required to sit before it gets allowed to go flying? And how is it protected?

And so the whole concept of that issuance of that number string is actually an issuance of an assertion string, and I'm told I can release it. It can sit in my repository in my laptop. If somebody gets my laptop and hacks my user name and password, they could be me. Or they could have it plugged into a USB thumb drive that you've got to carry around on your key chain or on a smart card, so that that process is the credential issuing process.

The interesting thing is a technology like SAML doesn't require PKI. It does the same thing. You do the authentication. The authentication then releases a SAML assertion that tells the other system, Brent just completed the authentication. Now there are advantages to PKI because it does digital signatures and other things, which SAML can't do. I mean, there are reasons you would use one over the other in an implementation. But understanding that the thing you get is a number, and you've got to have a rule set around what holds that number and then what releases it and uses it is key.

David Lansky – Pacific Business Group on Health – President & CEO
We're going to wrap up with our last. Our last question will be our mantra from Farzad.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Same question, what's the absolute minimum that we need to do to enable secure, authenticated, health information exchange, identity proofed and authenticated?

M
My recommendation is that you separate out authentication and identity proofing, establish the requirements around those using existing standards that are established by U.S. federal government EU organizations, and then look at the individual business processes within the healthcare industry: patient access to data, provider access to data, patient access to family member data, administrator access to systems, and you say what are the requirements for all of these business processes.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Let me simplify it maybe for level three that enable any doc. Let's focus on the physicians right now. Any doc, including then Spearhead, Montana, to be able to be identity proofed and authenticated to level three. What do we need to do?

M
So the minimum you do is you do nothing at all, and the marketplace will figure it out, and there'll be some bad compromises, but in the end it'll work, and it will. It always does. If you want to kick start this, and no one is going to like this – if you want to kick start this, you do it the same way you do it with prescription pads. The government issues credentials to physicians and the Department of Justice says that if you misuse those credentials, we're putting you in jail. That's what you do. If you did that, if every physician had a credential that they protected the way they protect their physician pad, this would not be a problem.

Our problem would be which technology are we going to use. But the problem would not be how to identity a physician. I know that's a tough thing. I know we don't like doing that in this country, but we do it with physician pads. We do DEA numbers, so there. Make the DEA number, you know, have the DEA be the issuance of identity for a physician.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
Other minimum suggestions?

Mollie Shields-Uehling – SAFE-BioPharma – President & CEO
I mean, maybe I'm sort of based on our experience in the sort of life sciences sector and what we're doing, maybe I'm missing something here, but we really believe that the processes are in place today. You can credential physicians. We are credentialing physicians. Our member companies work with them every day, and it's done through a variety of processes. One is this online antecedent process. Another is by work with the National Notary Association that sends a notary to do face-to-face. There's enterprise wide vetting, so for a large medical institution, you could do it that way, or you can do it through trusted agents.

I mean, everything is in place today. The providers are here. The processes are here. They're codified. The U.S. government has it. Again, we maintain that what is lacking today is a framework and a clear signal to the broader NHIN community about what is required around identity management. But again, they're all here. Certainly when you do an analysis of existing costs versus the potential rewards of moving to an online business, it's all in place. It's ready to go.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you all very much. It's been very helpful for us. I'm sure we'll have a chance to talk with you again. All right. We have one more panel. Thank you all for your patience, and I think we're gradually refining our understanding of this. Hopefully you can help us. As Farzad just said, dig a little deeper into the things we've missed so far. We have four more presenters, one of whom I think Sean will be by phone, if I understand correctly.

Sean Nolan – Microsoft Health Solutions Group – Chief Architect
Yes, that's correct. I'm here.

David Lansky – Pacific Business Group on Health – President & CEO
Great. Thank you, Sean. We have you, Sean, on our list as the third of our four presenters, if that's all right.

Sean Nolan – Microsoft Health Solutions Group – Chief Architect
No problem at all.

David Lansky – Pacific Business Group on Health – President & CEO
Again, thank you, gentlemen, for joining us this morning. I think you've now seen the drill. We'll just jump in. I guess, Frank, you're listed first. Is that all right?

Frank Villavicencio – Kantara Initiative – Identity Assurance Workgroup Chair
Yes, and I will torture you to please pronounce my last name. I won't do that.

David Lansky – Pacific Business Group on Health – President & CEO
Sorry?

Frank Villavicencio – Kantara Initiative – Identity Assurance Workgroup Chair
My last name, that is a test of your … abilities, but thank you very much. I'm Frank Villavicencio. I represent on behalf of Kantara Initiative, specifically a workgroup called Identity Assurance, and I'm also … another workgroup called Healthcare Identity Assurance within Kantara Initiative, so we're very grateful, very thankful for the opportunity … I believe is the shortest written testimony. Hopefully you appreciate that, and I'll try to do verbally the same service. I'll try to keep this very focused.

You would find that our testimony is a little different. We're not answering specific questions because our value is a little different. Kantara is an industry consortium, about 120 organizations, many within the U.S., and globally, a lot of Europeans, a lot of Australian, and even in the Asia region collaborating to define standards that help to advance privacy, identity management, interoperability frameworks that would allow more online transactions to occur. By definition, our focus is not industry specific. In my workgroup, I had the pleasure of working with David Temoshok, with Peter Alterman, with Rich Furr from SAFE-BioPharma, and a few others that are sitting here before you. So we have a very broad representation from multiple cross-sections of the industry, and we have taken on a very interesting task.

We have become almost a purpose now, which is to try to address and come up with a framework by which you can establish in a way that you can measure confidence levels that translate effectively to assurance levels. That way you can then go on to solve bigger problems like we're talking about today: enable electronic healthcare, record exchanges, and so forth. But likewise, we're also faced with similar use cases that deal with financial transactions or protecting sensitive data in, say, a DoD scenario and so forth.

We have come to a conclusion is that, as a cross-section of the industry, everyone seems to converge on this notion of different levels of identity assurance. And not to your surprise, we have actually started our work based on OMB memorandum 04-04 and NIST 800-63 special publication. We've collaborated with those entities, especially with NIST in the latest rounds of revisions of that standard or that guideline. Now what we've done is we've took those documents as a baseline, and we decided that to make this an operating program, something that could be actually coordinated, can be stand up as a program, there were other components that were necessary, so we've stood up what is now called identity assurance framework. This is a program that was launched last year, and it has four pieces. Now I'll read a little bit here.

On the one hand, we actually take the NIST and OMB definitions of identity assurance, and we go, what I will say, in a little more detail in prescribing what they actually mean, what they actually are. In doing so, we've also taken perspectives that are not only U.S. government specific. We've taken into account European points of view. We've taken into account industry points of view, for example telecommunications and so forth.

You would find that our definitions are compatible and aligned with NIST and OMB 04-04. But we believe that they're a little more prescriptive. And on top of that, the next aspect of our framework is how do you measure this. Is there a way that you could practically stand up and say, I am a provider at this particular level, and for that to … to a relying party so that a transaction can be enabled? We've been able to do that through two elements of our framework. One is the service assessment criteria, and that has three pieces.

And I think, building from what was discussed earlier, the panel just before this, there are three aspects of that service assessment criteria. One is the strength of the credential itself, how the strength of that credential maps to an assurance level, so we address the issue of what – not necessarily prescribing technology, but what characteristics of that technology need to be met to qualify for that criteria. We also have a component of identity proofing, and so we actually do have criteria that would convey to what extent, what level of strength the identity vetting process has occurred. And then the third element is, and I think I'll address your earlier question, the ongoing operations, the operation and oversight that the organization follows to conduct their business, and so that is another component of the service assessment criteria.

For you to get credential or accredited to be providing a credential at a particular level, you have to have satisfied all those three areas at that level. That's one very important component of our work, but the component that I think makes it pragmatic is the next one, which is the assurance assessment scheme and the certification program. Now we have an operating program. The program addresses two actors. One is an identity provider or the credential service provider, and the other is the assessor or the auditor community.

The intention of the program is to accredit the assessors so that they are competent, and they're qualified to assess based on the criteria we've defined. Then when they complete an assessment of a credential provider, for that provider to submit evidence to this program that they have satisfied the criteria. At that point, the credential provider then gets granted the right to claim that they comply with our specific level of assurance for our program, so that exists today.

This is an operating program. We launched it last year. Right now, it's actually very encouraging that we see adoption in multiple sides of the ocean, and in a number of industry areas.

Let me just conclude with a couple of things that I'd like to highlight maybe just to build from what was said earlier. We have a program that I believe addresses a number of the questions that I've seen discussed here today, and to quote Peter Alterman, you don't need to invent anything. You could just leverage this program. It's available for use now. It is not a specific healthcare program, and so we think this is important for adoption sake that we have a best of breed approach that not only addresses use cases in healthcare, but it is a broad cross-section of the industry. It is technology agnostic, so you're not locking your community into a specific approach or whether it is PKI or SAML. We're not really prescribing or locking any particular technology.

It is compatible with your government specifications and standards that have been discussed, NIST and OMB. And, more importantly, it's currently under review by the ICAM program, the identity credentialing and access management program by the federal CIO. And if we complete that application, we'll be the first trust framework service provider that would have completed that program in the government. So that should give you assurance or at least some comfort that we're very closely aligned with the federal requirements.

Then the last point I'd like to make is it has already been tested in a number of related scenarios. I listed some in our written statement. Several health information exchanges have taken our framework and put it to practice in some proof of concept. States, for example, Connecticut, Michigan, Minnesota, Nevada, Ohio, and Texas have successfully proven that by adhering to this common standard, you could broker trust in these payer systems in a distributed fashion.

I think that the work that's been done in the Michigan Health Information Exchange in particular is further along in implementing this, incarnating, adopting this program so that you could really scale the reach and ability to have credential providers in your network. Thank you.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks very much. Mr. Matthews, thanks for being here.

Michael Matthews – MedVirginia – CEO

Good morning. Nice to be here with all of you, and thanks for the opportunity. I think I'll begin my remarks today by taking exception to one thing that Frank just said. He in fact has the second shortest written testimony today.

David Lansky – Pacific Business Group on Health – President & CEO

We appreciate that.

Michael Matthews – MedVirginia – CEO

My … as being the shortest written testimony today. It is a pleasure to be here and represent the HIO's viewpoint on authentication. And we have a perspective, both through our participation with the Nationwide Health Information Network, as well as years of experience running a local HIO.

I'm glad that you had the opportunity to hear Dave Riley earlier this morning. I'd like to build off of some of the framework that he suggested where he talked about internodal health information exchange and intranodal health information exchange. We, in fact, are in the business of doing both. So I would lay out that you could view our work is at four different levels of authentication.

First at the NHIN and the work that we do there, and certainly call attention to the NHIN coordinating committee under Mr. Borland's fine leadership. Then we have our organizational level with MedVirginia as an NHIE and HIO. We then have practice level authentication through our client services agreement, and then we have individual user level within a practice. Within the user agreements are three different levels or roles at that point. You could have a physician role, a nurse role, or a nonclinical role.

At the client services agreement, this is the basic agreement that is signed by every practice that is participating with MedVirginia. There are 120 practices in the greater Richmond, central Virginia region who have signed the client services agreement. The responsibilities under the client services agreement are delineated in general terms on the testimony that I provided here.

The terms of use are then signed by the individual users, again, within the role that I just specified, either the physician, the nurse, or a nonclinical role. And this has all of the users responsibilities around use of data, security of passwords, patient privacy, and the like. There are 1,100 individual users who have each signed a terms of use.

In those agreements, in addition to how data are used, it also prescribes if there is any data supplied to the system in the form of clinical documentation, if there's a medication update or a vital sign input into the system. It prescribes how that information is provided as well. The principal, large data suppliers that we would have, such as hospital systems and reference laws, do have a data supplier agreement that speaks to the responsibilities of both MedVirginia and the data supplier in terms of data use quality, data mapping, and so forth. All of our data are audited at every single level. There are standard as well as ad hoc reports we identity at an individual user level and, within an individual user level, what patient charts have been accessed, how long they've been on the system, IP addresses, the results that any particular user has viewed, and so forth.

The physician, before any physician can come onto the system as a user, we do verify that that physician has a valid license to practice medicine in the Commonwealth of Virginia by querying the state medical licensure board. Before any user is issued a password and user name, there is training required for that individual before they come on, and the requirements of the terms of use and the client services are emphasized at that point.

For a physician to be able to access the clinical data on any given patient, there has to be an established relationship with that patient. That can be established electronically by the patient appearing on the physician's list of patients if we have an interface with the practice management system. It can also be picked up through the record of the physician being an attending physician or having ordered some tests such as a lab on that. If there is not such an electronic establishment of a relationship with the patient, the physician can self-declare a role and, as always, that is audited. And the physician specifies their relationship to the patient, the role as a physician, and what the intended use of that information would be.

We do have one other level. It's not really authentication, but it is an extra step. We do have the capability to put certain, particularly sensitive, clinical information behind the break the glass functionality so that the physician would have to then declare that that information would be needed. The area, as an example of that, that we have behind the glass would be HIV diagnoses, lab tests, and medications.

We certainly view these types of deliberations as a vital role, leadership role of government. We really appreciate the setting of standards for organizations such as ours that we're all adhering to an appropriate level of authentication, and certainly for us to continue to engage in the Nationwide Health Information Network exchange, having this kind of conversation, and the assurance that others are likewise holding true to that level of authentication as part of the trust fabric that's been spoken to earlier. Thank you.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks very much. Sean, if you're still with us, you're up.

Sean Nolan – Microsoft Health Solutions Group – Chief Architect
All right. Fantastic. I hope you all can hear me all right. First, I want to say thanks to the workgroup for the opportunity to participate today, and I'm sorry I'm not there in person. I had some, over the holiday, logistical challenges that caused that to not be possible.

I'm speaking here today as chief architect of Microsoft Health Solutions. It's a vertical group we established about five years ago to create both enterprise and consumer solutions to improve health and wellness. Of course, identity and authentication management are critical pieces of everything we do, and I am hopeful that our perspectives will be useful.

The first thing I wanted to cover is basically talk about what I can't cover today, I don't think, which is, there are many different types of identities and trust relationships involved in something distributed like the NHIN and providers, clinical users, organizations, patients, both as users and subjects. We've talked about a number of them. I think they all deserve their own discussions, but for me to cover them all in the time I have here would not be possible.

Instead, I'm going to focus on two specific use cases that I think really have the highest potential to engender confidence, both from citizens and providers, in the NHIN and thereby hopefully accelerate how we get to meaningful exchange. In particular, I really don't plan to talk much about authenticating end users in clinical systems behind the endpoints. I actually believe that attempting to institute a nationwide federation of clinical end user identities is really not necessary or even desirable at this time. It's not to say there aren't important and real discussions to have about authentication within clinical organizations, and it does seem clear to me that broad adoption of claims based access controls technology will greatly improve our ability to enforce things like local policies role based rules, but it's simply an issue that I don't think needs to be solved in the context of the NHIN itself.

What I think really our first thing is I do think is super important is organization-to-organization authentication because there really is no large, distributed system in the world where inner organizational trust is really global, especially with healthcare. This is rarely a technology issue, usually about local policy differences, regulatory variance and, frankly, simple business competition issues between providers that contribute to make multilateral trusts very often a near or absolute practical impossibility. I think that we really need to use organization-to-organization authentication and authorization for sharing patient records using some kind of system that enables point-to-point trust, something like hospital one and two agreeing to share summaries between them, as well as more rolled up relationships like a hospital agreeing to respond to patient inquiries for any organization that's been approved by a body, for example, CMS.

As it turns out, the Internet community already has a technical model that supports this full range of scope trust, the certificate authority hierarchy that drives commerce on the Web. By using the same digital certificates issued by known authorities to authenticate both sides of the conversation, together with purely local configuration of end points as to which certificates they will accept and for which purposes, I think we can immediately jumpstart a whole bunch of secure and private data exchange. There are two key points here relevant to things that have already been discussed today. I think, number one, this model really relies on the organization certificate or certificates as proxies for local org-to-org policy decisions rather than trying to code all that variance into the protocols themselves. For example, we talked about sending details of end user authentication methods in the envelope of a request. I think doing that is very, very hard to future proof, and it's very easy to get overly complex, and it's very natural for us to pull something like that level of decision out of the protocol and rely on that proxy of the cert. I know who I'm talking to, and I have local rules about what they can do.

The other thing about using an open authority model is that it allows for different levels of and, in fact, business models behind verification procedures and their rigor, and we've talked a lot about the cost of different levels of that today. Again, if we allow different providers to provide different levels of service, we do another good job, I think, to future proofing the system as best practices of all. Given that our first recommendation for government action is that we simply specify the use of hierarchical digital X-509 certs as the basis for organization-to-organization trust on the NHIN. And while we believe that any authority should be able to grant certificates for use on the network, a federal body, like HHS for example, should kick start that process by standing up a first authority to grant certificates, either directly to organizations or, if we believe that's too high cost, perhaps to the states who can then issue next level certificates to organizations within their jurisdictions.

The second piece that I really wanted to touch on is about patient identity and authentication. We know it's a stated goal of the NHIN to enable sharing of information, not only between organizations, but between organizations and citizen patients as well. And in order for citizens to be able to safely claim their own health information through the NHIN, it's super important that identity matches be perfect rather than probabilistic. This is a little bit of a new issue. It's not acceptable for me, as an individual, to be granted access to health information that actually belongs to the other real person, Sean Nolan, who lives in Belleview, Washington, as well.

This is a problem because all patient identity matching in the current NHIN specifications relies on probabilistic demographic matching. It's a powerful technique, especially absence of identifiers, but it's one that, by definition, always carries a non-zero error rate, and this is an issue even beyond the proofing issues discussed earlier because we don't have and are not likely to have a shared patient identifier that would allow us to reuse that proofing effort across nodes on the NHIN.

In today's world, the only truly reliable method for tying citizens to clinical records is an organization-by-organization match based on an in-person … proofing encounter. While at first it certainly seems a high burden, I really don't think it turns out to be the case. By regulation, patients already must made a documented request to receive their information, and certainly they visit their providers in person to get care, so it's a relatively simple matter to piggyback the proofing process on top of these existing practices. Given that, our second recommendation for government action is to resolve this gap in the current NHIN specifications by augmenting the current patient matching algorithms specified with a perfect match alternative that can be used by citizens to claim their information from organizations participating on the NHIN.

Both Microsoft HealthVault and Google Health, among others, already use variants of this mechanism to link patients with arbitrary clinical systems and further information about that is online. I think we really could translate those same patterns into something that would accelerate citizen availability going forward. And so with my high speed talking, which I wanted to do, that's my testimony. I look forward to questions and the conversation.

David Lansky – Pacific Business Group on Health – President & CEO
Very helpful. Thank you, Sean. And we'll now move on to our last presentation from Dr. McCallie. Thank you for being here.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. Thank you to the committee for this opportunity. My name is David McCallie. I'm a long-time associate of Cerner Corporation in Kansas City. I'm also a member of the standards committee. I have submitted fairly lengthy written testimony with details, so I will just briefly summarize some of our experiences at Cerner in dealing with some of these issues of distributed identity management and authentication. And I'll do it with the thought of here are some real world experiences to just oppose to the theory and the really profoundly powerful technologies that we have available to us that we heard about earlier in the morning.

Cerner, as you know, has facilities all around the world. I think we have one in Spearfish, Montana, although I'll have to go and verify. In our facilities, we give, in the EMR implementation – let me focus on that use case first – we give our clients the opportunity to add whatever second factor or strong factor authentication they would like to, ranging from fingerprint readers to RSA tokens to smart cards to badges, etc. And I queried the team that does that work for our clients, and they felt that they are pretty comfortable that it's less than 10% of our clients opt for any type of second factor authentication. I went back to them several times and said, are you sure … that number? And they said, well, it might even be less than that, so it is uncommon in the real world for physicians inside the institution anyway to use these additional factors. And the issues that get raised are complexity, cost, legacy systems that can't interface with them, but first and foremost, it's the burden on the productivity of the provider. I don't think that's a surprise, although it was a surprise to me, the numbers.

Cerner Systems support federated authentication to an enterprise within an enterprise using a variety of mechanisms that have been discussed this morning, SAML and LDAP and others, but we find far and away the most common approach to intra-enterprise authentication sharing is single sign on via screen scraping. Once again, the driver is that the hospitals have so many legacy systems, which don't speak these modern protocols that screen scraping is the lowest common denominator, and that's actually what gets used. My team, very informal survey done over the holidays, so take it for what it's worth, was that probably only about 30% of our clients even leverage that technology, the low level screen scraping.

Shift focus now towards non-provider, but really towards community, including non-physician users of the system such as administrators of our hospitals. We established recently an internal blog, wiki, social networking service that is designed to pull all of our clients into shared conversations with the Cerner associates who develop the software and with our third party suppliers who help us to deploy the software. We call it UCERN. I don't know that I like the name, but that's the name that stuck, and our goal was to get as many of our clients hooked up and registered in UCERN as possible, to do it as quickly as possible.

We initially tried to do that via a federated authentication model where we would take the Millennium user database, the people that use our software, and automatically grant them trust relationship into UCERN. It was a dismal failure, not for technical reasons. We were able to get the code to work pretty easily, but for what I would call identity granularity mismatch. The number of the people who were authenticated into one system weren't the same people who needed to be authenticated into the other system, and to solve that problem would have required us to create fake or dummy accounts in an EMR system just to get access to the social network and would have confused the boundaries of what kinds of information should flow. Should patient sensitive information be allowed into the social networking service, and so on?

What we did as an alternative, we stepped back and said, well, the e-mail addresses assigned to the users of our client's e-mail system is a pretty rigorous and trusted identity. It's certainly not as strong as some of the things we've been talking about this morning, but our clients are very careful in the way they assign their e-mail addresses, as I'm sure every one of the organizations that we work for today is, so that if every one of you in this room gave me your business card, there's an e-mail address on there that I would have total trust that I could use to communicate with you. So we decided to leverage that model for building this UCERN deployment where we create a white list.

If they can register, we ping them back with a message to their e-mail address to prove that they own the account. And then they complete the registration. It's quick. It's simple, and I believe that starting in July, we were able to; we've got over 1,000 clients who have activated that relationship and over 16,000 authenticated users. So the process works well for that particular use case, so it was leveraging a kind of trust, the e-mail address.

Let me speak now a little bit about patient authentication and connection. I believe one of the earlier panels made the suggestion that the provider could drive the identification of the patient. I think that's an interesting idea, kind of how our system works today. The consumer who wants to get a message from the provider via a secure channel has a registration process at the front desk where they establish a shared secret. The message is sent to that patient's ordinary e-mail address. They log onto a secure Web site, prove that they know the answer to that secret, and establish that relationship to that provider. It works well because if they already have relationships in our system to other providers, they can just add the provider to their current PHR account. It's still somewhat cumbersome, and it does put some burden on the front desk, but it's a simple model that does leverage the fact that the provider knows who the patient is.

You asked the question about directory services and integrating with outside directory services. I'll describe the problems and the successes that we've had with SureScripts integrating to our e-prescribing system. Nothing special here, but the issue is again this identity granularity mismatch.

The way that SureScripts identifies providers and what is the definition of a provider in their system doesn't match the way Millennium identifies providers. Neither is right or wrong. They're just different, so the mapping process between those two directories is non-trivial. It is currently done by hand and requires, in some cases, some cumbersome workarounds where we have to create pseudo identities in our system to match to what SureScripts expects in their system.

The use case would be a provider who works in two separate locations. The return request for a refill needs to be location specific, so that identity is de-normalized into the provider's directory by SureScripts, but that's not how Millennium sees it. We see just the provider's identity, so provider granularity mismatch, I think, is an issue that needs to be wrestled with.

Let me skip to the question of what should the role of government be. I'm going to give you a use case that I would like to see us be able to solve in the near term, knowing full well that the long range solution to the NHIN is something that we should keep in our long range radar, but the near term solution is how can two providers securely share patient information a push manner where one provider sends something critical to the other without having to resort to complicated procedures to assure that the security and privacy of that message, as it flows. The use case is one of my colleagues came to me and said that one of his patient's lab results came back late in the day. When he saw the numbers, he knew the patient had to go immediately to a local emergency room. He wanted to wrap up the data in his Cerner EMR and send it in a file, in a message to the physician in that ED describing this patient's fairly complex medical history, and he wanted to know if he could do that with regular e-mail. I of course said no, you can't do that. That's unencrypted. That's an unencrypted channel. It's not secure.

I suggested a cumbersome process where he could zip it up, put a password, text the password to the physician in the ED, etc. Ideally there would have been a local RHIO that everyone was connected to, and the data could have been pushed through there, but in our Kansas City region, there are at least three competing organizations trying to establish that footprint. Neither the sender, nor the receiver was a member of any of those three, and my bet is that it will be several years at best before that issue is settled as to what is the local HIE and what connectivitis should exist.

The simple proposal, which goes under the name of simple interop, and I'll be straightforward. Wes Rishel and I have collaborated, along with Sean Nolan and some others, in thinking through this. Could we create organization-to-organization trust at a mail server level using secure, mutually authenticated TLS between the mail servers, such that the locally assigned e-mail identities of the critical resources such as the providers could be leveraged to create this secure channel without requiring the top down management and issuance of all of these sort of top down managed identity that we've been hearing about this morning. This proposal would certainly be a stepping-stone towards a more widespread pull model where the proof of your entity needs to be stronger because you're not dealing with known personal relationships. I think I'll stop there and shift to questions.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you very much. Let me ask our panel for questions. Farzad has one.

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
David, I've been enjoying the ongoing blogs and the updates on the simple side interoperability string. And I guess it seems that the model you're talking about is one that could evolve into the full end user authentication, level three assurance if the organization that gets that certificate then assumes responsibility for identity proofing. So the model might be that the organization might be a hospital that then assumes responsibility for identity proofing the providers, or it might be an EHR vendor to small provider offices. When they're implementing the system, does identity proofing, you know, let me look at your drivers' license to make sure you are a physician before I implement and install your system. Could you comment on that possibility of having the delegation of identity proofing even to some of the level

three assurances and credentialing being done at those organizations that are the hubs in your simplified interoperability model?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. Thanks for that question. I think that's exactly how it ought to work. I think the model is layered on an assumption that push messages are typically between people who already know each other and trust each other, so the primary issue is the security and integrity of the message as it flows. That, in most organizations, already exists in the form of e-mail addresses and could be converted into secure e-mail addresses following the same process that they allocate e-mail addresses.

Going from that to a pull model where you're aggregating data about a consumer and an as yet unknown person in the future who has not yet consented for access, so you don't know who they're going to be. When you move to that model, you have to ratchet the level of trust up, so the simple proposal is start with something that's not controversial, and eventually let's move to a more difficult level of authentication. But I don't see any reason why they're incompatible. I think that process could just be stepped up, and I think we heard this morning a variety of ways to do that. So I may not have answered your question, but I think the answer is yes, it's a natural progression, and it does leverage, as Sean said, the organization-to-organization trust as the starting point, and then it goes from there.

David Lansky – Pacific Business Group on Health – President & CEO
Let me ask … before we go to, I think Wes has a question, anyone on the phone of our members want to get in a question? We neglected you. If not, Wes is up.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
I suppose I should make some comment about that clown you're collaborating with. I'm wondering if you would agree with me that the more – David, I have learned over the last couple months that he's a black and white person. I'm a shades of gray person, so I'm about to go into some nuances here.

The push model kinds of bleeds over into a gray model, into a pull model if you push a request and then they push a response back. In that sense, for example, the work that Social Security Administration does falls into that model. Would you agree with that? I'm leading the witness here.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. Again, is that an automated response or is that a human mediated response, obviously different requirements.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Right. And we, at a minimum, require that the operator of the IT that implements these PLS … mail servers and the HTTP servers and so forth meets some criteria, not yet established, to be trusted to operate that thing, so we're specifically not envisioning all the practices in the country operating it. We're expecting them using either their vendor of their EHR or some entity we've thought to call the health information services provider that achieves that certificate. In whatever that method is for accrediting those entities, we could apply the processes we've heard for accrediting them as identity proofers as well. Is that…?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right. The nodes would be required to go through a fairly rigorous process, which eventually involves obtaining a certificate from a designated authority. The end users would have to follow a policy driven process, much as we've been discussing all morning as to what exactly should that policy be and what are the fine points of how rigorous it should be.

I think that it could be less rigorous to start with if the use case is confined to the push models because of the fact that that tends to be between individuals who already know each other, trust each other, and are engaged in consented care. In other words, they're fulfilling the duty of an already agreed upon care process. That's a somewhat lower standard because the abuse potential is so much lower.

I thought Sean's point about probabilistic matching and patient identity is absolutely critical too. It's the invisible 800-pound gorilla in the room worrying about authenticating the providers when we don't know who the patients are, so it's all levels of probability that we're dealing with. The NIST levels are a great way to segment that. I look forward to the revised version that breaks it out into more detail. I think that the use of intermediate tokens like the cell phone makes tremendous amount of sense as a fairly noninvasive way to radically increase the security of the conversation. I think that's a terrific idea.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Frank?

Frank Villavicencio – Kantara Initiative – Identity Assurance Workgroup Chair
One comment because I think this is a very pragmatical discussion, which is very engaging. When I hear your use cases, immediately in my head I'm thinking this is mostly at level two assurance problem. In our workgroups, we wrestle with the practicality is that you go through different levels of assurance at all times. You don't need a strong credential every time, and so there will be triggers for you to go from one level to the other. So when you now think about how you go from one level to the next from an end user standpoint, the rigor is the delta, which means, as you said, there's established trust. There's some baseline, and all you need to worry about is how you go from that baseline to the next threshold. And so by approaching it that way, you simplify the end user experience, hopefully reduce cost, and achieve more scalability.

There's a comment from the last panel, a gentleman from Anakam, which I think that the levels of assurance tend to intimidate sometimes. I think that's been my experience. Level three, I think, is mystified as being unattainable, unachievable, and not able to reach Internet scale. I'm for one a believer that that is not the case at all. I think that if we demystify that, and this could be a way of doing that, you will find to be less invasive and possibly a more likely adoptable level. That was my point.

Sean Nolan – Microsoft Health Solutions Group – Chief Architect
I'd love to throw something in if I might. I don't want to interrupt. It's hard to know from the phone.

David Lansky – Pacific Business Group on Health – President & CEO
You're fine. Go ahead.

Sean Nolan – Microsoft Health Solutions Group – Chief Architect
Yes. I just wanted to reinforce one thought too, which is that as you start to think about how those institutions do get their certificates, and what they have to do to get them, there are two issues: one that Farzad brought up of delegation I think is really key in making that manageable. I think number two is it's not necessarily a problem that we have to solve once or for all time. This idea of having many authority providers, just like we have many consumer advocacy organizations in the world, and people trust different ones, could be very powerful to say that for point-to-point or region-to-region communications, there may be sharing, and they may be able to work out policy and those types of variances between each other very easily and share even a single, frankly, self-signed certificate, although that might be going too far. But the point being, an open set that allows for different levels that each institution gets to

choose, do I believe that that rigor was sufficient for a particular transaction, as you go from the different ones, the push, the pull, to the individual ones and so forth.

David Lansky – Pacific Business Group on Health – President & CEO
I think our brains are fully saturated, and we'll need to get some fuel to process all that, and then we'll come back. I think we have an opportunity now though, and so if that's all said, no one on the phone has a question, we will adjourn this panel, and thank you very much, again, for making the time and trouble to come help us today.

With that, I think we have an opportunity for public comment. Are there any people here in the room who wish to give us comments? It looks like there are. Judy, is there a microphone for today? Your mic wasn't on. Hold on. Do all that again.

Judy Sparrow – Office of the National Coordinator – Executive Director
On the telephone, if you wish to make a comment via phone, please dial 1-877-705-6006 or simply press star, one, if you're already connected. We'll begin in the room with you, sir, if you would please state your name, your organization, and please keep your comments to three minutes. Thank you.

Chris Penny – TNS – SVP, Head of Corporate Development
Three minutes. Okay. Thank you very much. Hello. My name is Chris Penny. I'm Senior Vice President, Head of Corporate Development at TNS, Transaction Network Services, based here in Reston, Virginia. TNS, just from an information perspective, is a global communications company that provides and manages telecommunications infrastructure that the payment industry relies on to securely transport ATM and point of sale transactions. The financial services industry relies on to securely transport electronic trades and related information. The telecommunication carriers rely on for SMS, caller ID type of transmissions.

On a monthly basis, we transmit over a billion transactions a month of POS and ATM transactions, as well as electronic trades and telco related messages such as SMS and caller ID. We have over two billion devices disbursed geographically, connected to our networks, that's connected to our customer's networks. So we run our infrastructure on a community-based network, enabling participants to cost effectively and securely interact and transact with each other. We manage interoperability issues between those customers associated with multiple standards and protocols, etc. In each industry we operate, we accept all sorts of transactions, and all sorts of participants that participate in our community of interest.

There have been three common themes that have been discussed: trust, how do you build trust in the system from an authorization standpoint, and then using existing technologies today. We've been in and around these industries, payments, telco, as well as financial services that we've seen the evolution of similar networks, and we have three recommendations that this committee, I think, should consider when you talk about authentication.

First of all is run an intelligent network via an Extranet with the centralized registry approach. Services such as authentication, security, and privacy can be managed in the network. It can be managed in the edge, as well as in the network. In healthcare, you've built monolithic architectures that exist not only to support information. There's no interoperability associated there. The managed network can take care of that interoperability much like we do in payments.

A registry approach will allow participants to effectively exchange data between each other without the cost of associated building these huge, centralized data farms. Additionally, it also alleviates the privacy concerns about having a centralized data, and you can more manage remotely manage that data between participants point-to-point. More pertinent to today's discussion, as you sent levels of authentication outside the edge, a registry approach will allow you – a registry and a private Extranet allows you to manage who can talk to whom based on what level of authentication and what data that can then be transferred between point-to-point. The registry, a central registry like we run in telecommunications allows you to do that.

The second point, bridge the technology gap. Bridging the technology can be done. The NHIN should bridge the legacy solutions that coexist today with evolving innovation. The healthcare industry is a complex environment of varying standards and protocols. We all know. It could take decades to implement global standards. We've seen this in the payments industry. We've seen it in the financial services industry. But as we've seen it in the financial services industry, a standard protocol such as FIX has been adopted that allows electronic communications, not only nationwide, but globally. What's also important is the establishment of a single protocol does not mean there's one Extranet. There are many Extranets out there competing today in the financial services world to provide electronic trading securely on a cost effectively basis and with remote latency, with latency as an issue.

Lastly, I think the thing that the committee needs to consider and allow this from a business perspective is that sustainability and scalability is critical. Remote authorization, we've talked about can happen in the HIE world. The problem is, in the HIE world, the scalability of that business is going to be very difficult, as you grow from a small, regional area to get scale. Enough transactions, you're not going to be able to scale that business where that's going to be a sustainable growth model. So we agree that remote authentication can happen in the HIE thing, but the problem is to get enough transactions across that business to allow that business to grow.

We've seen this before in the ATM side 30 years ago, how many ATM networks were there 30 years ago versus today. So just consider that scale is a big issue, as you think about authentication, as it relates to this from a private Extranet standpoint, from a legacy standpoint, and then from a business standpoint. Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Ma'am?

W
Hello. My name is … and I'm a software engineer developing….

David Lansky – Pacific Business Group on Health – President & CEO
Can you move the microphone down a little bit?

W
…information … for more than 30 years. I see a big problem with the current situation in the proposed solutions is that the patient data is duplicated in many systems and, at the same time, a particular patient or health provider doesn't have access to the complete patient data. And the data and the difficulty of flowing between one system to another, some systems are fairly sophisticated, and other systems like a small doctor could be just a paper system.

Then I think, fairly clear, the solution not only for authentication, but for other reasons, is to centralize the patient record, to have a government sponsored or could be private government, but anyway, centralized system that centralize all the patient records, and also contains the information about the health providers and influence companies. Then, in that way, and also is accessible to everybody … free Web site that then when the patient goes for the first time to the health provider, like a small doctor, that doesn't have to pay to access a sponsored government site.

Put his data in the patient data belongs to the patient. Then he is going to authorize that doctor to access his data. The patient data and the health provider data is in this government system or government private, whatever, the centralized system, and is going to maintain this relationship between this patient has access, this doctor or health provider has access to the patient record. Of course, the patient has removed the access … to consider that no longer want to have a relationship with that doctor.

Then of course the doctor or health provider is going to add to the patient record any new information about the visit. Because the data is centralized, that information will be available to another health provider that is authorized by the patient, and really doesn't need to – you need to figure out how to interface from systems that have different kinds of capabilities because really the data is only one place, and different health providers or patients have access to that centralized data.

Judy Sparrow – Office of the National Coordinator – Executive Director
Could you sum up now please?

W
Yes. Basically I think a lot of problems would be resolved in a system that I'm proposing that centralized patient record and also health providers and other information that is needed to maintain the system.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you very much. Sir, you have the last word.

Michael McGrath – Gemalto
Hello. Good afternoon. I had to check to see what time it was. My name is Michael McGrath. I work for Gemalto in North America. We're a digital security company. In listening to the discussion today, there was a lot of discussion about identity proofing, and I want this workgroup and the policy committee in general to kind of think outside the box and not work in a silo as solely looking at healthcare in general.

There are a lot of identity initiatives going on currently. One of them is revamping the social security card. Senator Schumer from New York introduced legislation in the fall to have a biometric social security card as part of the immigration reform. That biometric social security card will require in person identity proofing. It will require the citizen provide a fingerprint, and it will bind that credential to that person.

The existing infrastructure is there to service millions and millions of people, and it's grossly underutilized today. The U.S. State Department utilizes the post office for identity proofing for the U.S. passport. That was discussed briefly today, but I don't want it to be glossed over. As we all know, the post office is running deep in the red right now, and they are trying to cross-train their existing workforce, and there's no better way to utilize that workforce and those locations to identity proof whether it's the consumers, the patients, or the providers. I just wanted to stress those points because the existing infrastructure is there.

The other thing is that early in my career, I was a stockbroker when I first got out of college. I had to go in person identity proof who I was to the police station. The FBI has my fingerprints on file because, as a stockbroker, that was a requirement to provide those fingerprints because I would be managing money. I see no reason why HHS can't mandate the same thing. If SEC, Securities and Exchange Commission, can mandate stockbrokers to provide fingerprints and do identity proofing, the State Department requires citizens to do identity proofing, it's logical that HHS can follow the same suit. Thank you.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you very much.

Judy Sparrow – Office of the National Coordinator – Executive Director
We have nobody on the phone, so back to Dr. Lansky.

David Lansky – Pacific Business Group on Health – President & CEO
Thank you. All right. Then we are fully prepared for our discussions this afternoon of how to move forward with recommendations based on the input we've had. I think, for now, we have a break until 1:30. We're exactly on time. We have until 1:30 for a break, and there was some discussion of there being some lunches available for purchase. It's not the case? Okay. So everyone is on their own for lunch. Be back here at 1:30. Thank you all. Thanks again to the witnesses for coming and joining us today.

My fellow panelists, while you're all happily munching, we're going to actually restart the formal session and be live on the Web, so be aware of what you may say may be broadcast broadly, globally.

Judy Sparrow – Office of the National Coordinator – Executive Director
Joe, you'll ask Chris to open up the public line.

M
You're already set, Judy.

Judy Sparrow – Office of the National Coordinator – Executive Director
We are? How long has that been going on?

M
For about ten seconds.

Judy Sparrow – Office of the National Coordinator – Executive Director
Great. All right. I think we're ready to resume the NHIN Workgroup Meeting. Dr. Lansky and Danny Weitzer is here, so please reconvene.

David Lansky – Pacific Business Group on Health – President & CEO
Do you know if we have anyone on the phone now, Judy?

Judy Sparrow – Office of the National Coordinator – Executive Director
Is anybody on the phone? Marc Probst, Marc Overhage?

Marc Overhage – Regenstrief – Director
Yes.

Judy Sparrow – Office of the National Coordinator – Executive Director
Pardon me?

David Lansky – Pacific Business Group on Health – President & CEO
Marc Overhage is. Hello, Marc.

Judy Sparrow – Office of the National Coordinator – Executive Director
Marc Overhage.

Marc Overhage – Regenstrief – Director
Hello.
David Lansky – Pacific Business Group on Health – President & CEO
Our intension with this next hour was to digest what we've heard, as well as our lunch, and see if we have at least some way of framing the authentication issues in light to today's testimony that we can begin to use as a way to populate the recommendations that will come forward in the next week or so, if we're able to come up with some. I'll be pleasantly surprised if anyone has fully processed all this and is ready to lay out a framework. We are iterating one up here. Maybe to start, let me just go around, starting maybe with the phone, with Marc, and see if anyone has any distilling comments they want to share based on what they heard this morning. Then after we've done that round, we'll try to put together some template to continue the conversation. Marc, since you're there, do you have any overall reactions to where we are in the authentication presentation?

Marc Overhage – Regenstrief – Director
No. No surprises. This is challenging. I do think that, and I can't remember which presenter it was, made the point. I think it's important to bear in mind about the approach and process for providers and for patients may well need to be different. I think that's a really important distinction we may want to make to Farzad's point of what's the absolute minimum we can do when to move forward. That's my only substantive contribution.

David Lansky – Pacific Business Group on Health – President & CEO
Thanks. Is there anyone else on the phone? No? Let's just go around, and let first committee members, and then other interested parties give their thoughts. Micky, do you have anything?

Micky Tripathi - Massachusetts eHealth Collaborative - President & CEO
No. I mean, I think certainly there were more layers to this than I think I appreciated before we started talking, and I was particularly struck by sort of that last inch problem of the identity proofing at the end of the day and how important and key that is. I will say that I think that there are a variety of ways that one could think about trying to make that more efficient based on different ways identity proofing has today, which could be maybe different from whether it's licensing or what have you. I don't think it's unreasonable to go down a path of saying that identity proofing, the face-to-face identity proofing is required, and that physicians ought to consider that they have to do that as a part of participating in health exchange. That feels to me like we do that in many, many other areas, and we're taking on a pretty big responsibility here, and I don't know why we would. You know, that at the end of the day, it doesn't feel to me like we should shy away from that.

David Lansky – Pacific Business Group on Health – President & CEO
Very good. Jim? I'm just going to go around the circuit to see if anyone has any. Now you're forewarned.

Jim Borland – SSA – Special Advisor for Health IT, Office of the Commissioner
I didn't realize this was serial. Yes. I think what I heard this morning was that there probably isn't a one size fits all solution to this problem, and that our framework has to accommodate individuals, as individuals, in say a solo practice physician. Individuals within organizations where there are existing trust relationships because of some sort of a relationship between an individual and an organization, employment or rights to practice, those kinds of things.

And then I think the other thing that we have to consider, and I'm not sure we heard it very clearly this morning, but what I'm calling NHIN business associates. This is the idea that information flow may not only be from provider-to-provider via the NHIN, but that there may also be intermediaries who may facilitate the exchange of health information, for instance, EHR vendors who may wish to stand up their own gateways to serve their customers. Where I think that's going to be especially important is in the software as a service realm. Not a one size fits all solution, and let's recognize that there are different trust models, and they don't all necessarily involve credentialing at a particular level of assurance.

Latanya Sweeney – Laboratory for International Data Privacy – Director

Okay. First of all, that was a really good session, and I really liked the lead off panel, the way that happened because I think they really set the stage nicely. Whether you agreed or didn't agree in the variations of things we heard … I think was really good, so I thought that was really good.

One of the charges I sort of heard in there was maybe it's a good idea to go through the meaningful uses or some other delimitation and figure out what are the right risk assessments here. What are the right levels, or do we just declare they're all level three and move forward, or might there even be variations within three if they were all considered in the space of three because there's patient information? But they're not always all patient information, so it's not even clear if they're all level three, and so kind of sweating that detail out.

There were a lot of issues, a lot of really great ideas and comments that came to mind about how one can use the context to leverage changes in security, something that went from what might be a level two to a level three, and they don't necessarily have to start over again, or maybe we do want to start over. That's a sort of question on the table.

Then there were a lot of good questions, a lot of good comments were made that started to put pieces together of tradeoffs if you choose this kind of, you know, if you choose a big, centralized model versus decentralized versus I have a sharing of standards. And there are some benefits and tradeoffs on each of those. And some of them are exclusive, so sometimes you may have to put a stake in the ground. It's not clear you can just sort of say I'll do all of them. Those were sort of my big takeaways.

Christine Bechtel - National Partnership for Women & Families – VP

Quickly, my big peak was that first of all, I thought it was great. I thought the format was really good, which was a little bit different than the first time around, and it was a very rich discussion. I liked it and agree with Latanya that having the federal panel first was very helpful.

I liked also hearing from MedVirginia as an HIE. I had the good fortune, and I don't know if SAFE-BioPharma would characterize it that way in the reverse, but I had the good fortune to collaborate with them on a paper two years ago about authentication, identity management, and HIEs. We talked to, I think it was, four different HIEs. Marc was one of them, both Marc's actually, Mark Frisse too, and what became clear was that there's a lot of variation in how they do and don't authenticate, and that they had some inherent strengths and weaknesses in their abilities to do that.

And so, I think my big picture takeaway is the obvious, which is, there is a need and, I think, a role for the federal government or the governance body of the NHIN to set some basic requirements for how providers who are going to participate in information exchange are authenticated because I think it's a little bit of the wild west out there.   And then the other thing, which is a smaller, but important observation, is I know that the Microsoft folks and a couple of other people on the panel today mentioned patient authentication. I think that's an area we could spend a lot of time exploring, and it's very interesting.

I think, as we think about authenticating patients, one of the areas that I want to make sure that I have in the forefront of my mind is the diversity of patients much like the diversity of providers, that it's definitely, I agree, not a one size fits all solution because I think there are a lot of patients who won't have access to the system, or won't have access in ways that we think they should. We want to make sure that we can facilitate things like online visits and multiple ways that patients can access the system, but doesn't always rely on an in-person visit to the office during strict office hours and things like that, so how we really be flexible and yet secure in the way that we approach that issue is important.

Neil Calman - Institute for Family Health - President & Cofounder
No comment.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
I'm sure we'll get into the discussion. I'll just make a few brief comments. Again, I felt like no big surprises, but I do think, for our own deliberations, it would be good to separate the discussion of provider authentication from consumer authentication with a very stark line because they're very different problems. I felt, even in the discussion this morning, things were getting blended in the discussion. I do think that the question of the authority for the organization that's issuing a certificate is one that we should grapple with a little bit.

M
…the authority for…?

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
The authority of the entity that's issuing the certificate.

M
We had a discussion about GSA having a list that was not a very useful list, and whether they're inadequate certifiers.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
Yes. I do think that's one issue, and I do also still want to go back to the question of how to leverage the national provider identifier as an identifying element in whatever this construct is because it may get us a long way there. We need to discuss that. On the consumer side, it's a much more complicated issue, and I do think there's been some progress in that area. At least, I heard it today, and when we're ready to get to that, I'd love to discuss that.

Arien Malec – RelayHealth – VP, Product Management
I heard a number of themes come out during the discussion. One is the need to keep the authentication and identity proofing process local and as close to the provider as possible, which I think drives certain policy and architectural considerations that the organization is doing the authentication needs to be, if not geographically, at least from a business perspective, have a close relationship with the provider.

Number two is the need to tightly couple the policy framework and the technology framework. That is, the technology doesn't give you anything independent of the policy and procedural framework that drives the authentication process. You can have all the technology in the world. It's going to drive down towards the weakest policy implementation. There's a need, I think, for a standard policy framework.

The third thing that I heard and that then I heard refuted is the notion that level three authentication, both from identity proofing perspective and from an authentication perspective, is easy, and there are all kinds of technologies out there to do it. And the only examples that we heard of real use of level three authentication were in employment relation – were examples of employment relations or places where there's a direct financial relationship because there's a contracting entity with the federal government who is required to do level three authentication. I didn't hear any good examples of level three authentication at the individual provider level. And, in fact, we heard from David that when the option is given, the implementation rate is extraordinarily low. I compared notes at lunch with those of us who were providing HIE services, and the examples are pretty much parallel down the board that there aren't great examples of level three authentication, so those are the three key takeaways that I took, as well as the notion of patient and the provider being very different beasts.

David Lansky – Pacific Business Group on Health – President & CEO
Farzad?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
I think the most interesting decision and kind of issue to discuss was in that last panel when Sean and David presented the alternative model. We had spent all morning talking about end user credentialing, identity proofing and authentication. And the model there would be you determine the assurance level for different uses, and for many of the things we're talking about where it's access to many, many patients. Harm could come to patients if information is misused and so forth. It's likely that it's going to be assurance level three requiring two factor authentication.

Then we heard that there would be essentially what we would need to do is to either establish a centralized process, the DEA. David Miller, I think, gave the example of the federal government issues credentials to every provider in the country, just, you know, if you want to accelerate it, that's what you do. Use your authority. Piggyback on DEA, and you're done kind of thing. Or we just say, hey, you've got to get assurance level three. There's a marketplace out there. Maybe there's an accreditation process that's more, that's better than the current, you know, how you get on the GSA list. But basically there'll be a marketplace of continually improving ways of doing identity proofing and authentication for providers, and that's approach A.

The advantages of that are that it is increasingly feasible to do this, although someone made the very good point that it's one thing to get the technology, to get the identity proof. It's another thing to have all the technologies you need to use being able to use that token. So I may have an HSPD-12 badge, but I can't stick it into my computer right now and be able to access all the Web sites I want to access, and be able to access my e-mail, and not have to use my password. So having the token and having the technology that the end user be able to use that token, the multitude of potential tokens is, I think, an important point to recognize.

That having been said, if we could figure out how to get every doctor in America tokened up, there would be multiple uses for that, everything from birth certificates and death certificates, emergency medical to controlled substance prescribing. There'd be huge, you know, it's hard to think that the future isn't going to need something like this. On the other hand, if we focus on our four core meaningful use stage one requirements, it's hard not to think that it's going to be much more feasible to get there in the near term by going to the accrediting and deeming of organizations who get the certificate and do the server-to-server TLS that David McCallie and Wes have been talking about in the simplified interoperability.

The other advantage of that, in addition to being much more feasible, is that it ties it. It's kind of a two-for. It also links into the routing mechanism of the information, so it's not just a credential that you get. It also carries implicit within it how that information is to be routed through the servers of the health information service providers.

Right now I can't process it all right now about how these two in our recommendations are going to come together because if we go to the logical conclusion of the set the assurance level is probably going to be three. Let me market rule. It could be years and years and years before that capability is going to be available to every provider who wants, motivated provider who wants to be a meaningful user in 2011 and 2012. On the other hand, I'm not sure if the server-to-server implementation takes us to get to that other endpoint. The only way I can see, and this will be my last thought on this, is the only way I can see this taking us there is if those health information service providers also provided identity proofing, either themselves or through partnerships with others where the EMR vendor also checks your drivers' license when they do the implementation in the one doctor office.

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
So I think one important lesson we heard that already was mentioned is that the evolution from the remote – we're really talking about remote authentication. That is to say, we're not so much caring how a user gets access to their local EHR. We care about how they get access or originate information that is communicated somewhere else. We, I think, all recognize that that communication is not always attributable to the overt action of a user. Sometimes the system decides it's time to send this information.

We also recognize that portals that may be operated by HIEs or PHR vendors or anyone else represent a classic case of remote access. Somebody in one organization is logging into a portal offered by someone else, and we need to know how to authenticate that. They were most specifically, most of them talking about being able to remotely access an application as a user, and one of their points is that it's not enough to have a credentialing system. It's not enough to have a – it is important to have a variety of authentication mechanisms. But it also takes refitting the application to be able to accept this level of authentication. And that's apparently a slow process, based on what we hear. It's apparently a significant investment of the people who maintain those applications to bring it up to that level.

I hope we can, however, perhaps go through the meaningful use criteria and distinguish those cases that are remote access to an application from those cases where the communications are really system-to-system, and the purpose of user authentication is to provide a reliable audit of that transaction. In other words, if I'm going to respond to some other, some hospital that sends me a request, and they say it was done because Dr. Smith made this request, I've got to have a reasonable level of comfort that if I every have to go and have that challenged, I'll go to them, and they'll be able to show me that, yes, well, it could have been anybody who said they were Dr. Smith or not, so I think that's important.

I think it's most important to support those cases that are needed immediately without tremendous retred of systems that have to use them. That is, I think that if we have a goal of achieving meaningful use, achieving meaningful use means getting interoperability. It's pretty limited for the next few years if it's only among a few systems that have been able to qualify as meeting meaningful use. If we really want – I mean it's my impression that interoperability begets interoperability in the sense that the more people use interoperable systems the more trouble they're willing to go to to be able to use interoperable systems and I'd like to see us make sure that we start at a level that maximizes that interoperability. Thank you.

Tim Cromwell – VHA – Director of Standards & Interoperability
This is Tim Cromwell. Just one quick point about identity proofing in person – a question really: The question is, is there something that would be called de-authentication? And what I mean by that is aren't we going to have to worry about those times when a clinician moves, a clinician retires, a clinician is de-privileged and if we have to worry about that then it makes sense to tie the in-person identity proofing

concept to the credentialing bodies, the state license facilities or the DEA. Every clinician goes and gets a DEA number. It makes sense that incrementally we can take an approach. I know, Farzad, you were worried about how are we going to give a token to every clinician, but you know, to have it be voluntary and tied to incentives somehow. Those are just some observations.

M

I have one thing. I just wanted to say it's not every physician. Tim said every clinician and it's an important distinction there.

M

Yes. A lot of the comments I would have made have been made, but a couple of things: I guess I'm almost ready to make my comments by asking several questions, but for me I keep coming back to this. I think this is about meaningful use of electronic health records, and so to Wes' point I think we've got to understand or to his last point is that a focus on interoperability or that small few that have electronic health records now and will over the next couple of years or is it about interoperability for all and trying to move interoperability and, therefore, having a solution that might be a different one. So I think we've got to think hard about whether we want to push hard on meaningful use of certified electronic health records versus having much broader interoperability that includes those that don't. That's an important concept here.

M

(Inaudible.)

M

Have electronic health, the rest of the country, the 80% that don't.

M

Eight percent of physicians that don't, right?

M

Right.

M

Right.

M

Right. So, because that changes your decisions here, so are we talking about meaningful use of electronic health records, which is how I come at this; but I also understand the pull and tug with interoperability and pushing that and getting more engaged interoperability.

The other thing is I'm struggling with the initial concept of the NHIN being a network of networks versus a network or a virtual network to allow interoperability for all of those locally or wherever because, again, that changes some of our decisions.

Then lastly, is this more about a provider-to-provider transition of care or transfer of care document and that type of thing, or is it more or partially about a look-up, because that changes our thing. So my comments are asking some more questions that I think need to be answered and figured out, because that will drive some of these answers.

M

Marc, do you want to weigh in ...?

M
Wes got to do this. I want to do it.
M
There are some things only Wes can do.

M
Anyway, again, to me it comes down very much to what's going to be the impact on the workflow to the providers that we're trying to get to adopt because, one, we don't want to discourage adoption and we also don't want to discourage those that do adopt to not do these things that get this next piece on interoperability.

Todd Park – HHS – CTO
... one, just takeaways; this is not a new problem. Secondly, this is not a technology problem. Very rarely is a problem a technology problem and so we should very assiduously steer away from anything that smells like a technology solution; A, because it's not the right answer; and B, because it also will lock in current ways of doing things that I think, as we've heard this morning, are evolving rapidly. Actually, given the fact that it's not a technology problem it really is a policy and business process problem.

Another takeaway that got burned in my brain; and I don't know if this is what everyone else heard; but it's very hard to solve the underlying policy business process problem without trusting/delegating the solution to the answer. So the charismatic fellow from NIH, the one who was part of the first panel, talking about the fact that if you think you're going to solve this problem without actually enabling or requiring that people trust something sent from someone that basically was deemed trustworthy by someone that you don't know, that just isn't going to work. But at the same time there has to be some kind of ultimate root of trust that comes from somewhere so that you have faith that this thing you've got from somebody, who is basically deemed trustworthy by someone you don't know, but you have faith that if something breaks down in that chain that someone is going to pay, right, that someone's neck is going to get choked so that, in fact, there is an inherent trustworthiness in the system that you can rely upon.

I don't know if that makes sense, but the whole notion of actually delegation of the deeming of people as trustworthy was an important concept that I kind of took away from it and that seems to me to be an important part of whatever solution that we come up with.

M
Mariann, do you want to join the comment today?

Mariann Yeager – NHIN – Policy and Governance Lead
I thought it was very telling that one of the initial, I guess, noteworthy comments that were made by the federal panel was the assumption that; and I'm just raising the awareness; that we really shouldn't jump to the highest bar in terms of the level of assurance, but that was sort of the natural assumption that folks made, particularly in the types of information exchange that are taking place within the NHIN today. There actually has been some discussion about level of assurance. There actually has been some discussion about level three assurance. But I thought one of the most noteworthy things that came out of that discussion was the recommendation of having a process for coming to a level of assurance and not jumping to just the highest bar, which I think is very important for this, for what we're talking about.

M
Great. I'll just add a couple of thoughts I had, which are a little bit contrarian to the direction we're going. One, which I did think that many people said was to be wary of the usual healthcare exceptionalism. This

is a problem that's been addressed in many other industries, including with higher standards and risks than we face even. In just my own personal experience, I think about Internet banking and so on and how much very large scale financial transactions are going on without even in-person proofing all of the sort of ... some very antecedent in-person proofing there, but maybe there are more lessons for us to learn by looking at some other industries.

I'm also struck, Carol, we looked at ... issue three or four years ago and there was a line in the Markle report saying, "Knowledge based authentication should be really good, but we have no evidence," and we heard again this morning that we still don't have the evidence, which is really puzzling.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
... person either.

M
Right.

Carol Diamond – Markle Foundation – Managing Director Healthcare Program
There's no data for that either.

M
So there's really the sense of having an objective metric against which to determine the risk really. We're speculating, so that's a little hard to make policy in that environment. But the contrarian thing, I feel, is that I tend to think that the provider issue is a subset of the consumer issue, not its own problem to solve, and I'm not very comfortable pursuing a short-term, separate path based on the idea that a prescriber is the distinctive competency which justifies someone to be a health information user and, therefore, on the network, which I think is implicit in a lot of our discussion. If we're going to enable lots of other kinds of health services workers, professional and otherwise, within 2013 and 2015, within a relatively foreseeable time period to be on this network not only as consumers, but as other health providers, we should at least architect our solution set with that as the primary outcome and providers may be a first instantiation of that and maybe there is some extra features that providers, because of their licensing and so on, have, but on the whole I'm nervous that we will build an infrastructure which perpetuates an institutional structure we don't much like and we should be wary of doing that as we define this first phase of solutions.

That was a very helpful, I thought, round robin. We just got a lot of good ideas out. Danny, thank you.

M
As usual, it's great to hear all of your insights and I'm sorry I missed this morning. I was at home with my own kid's healthcare issues, but they're better now. Thank you.

I think that I guess I'd just make one observation about what I think is a slightly new wrinkle in the direction of our discussion, which is the focus on intermediaries, which interests me quite a bit.

M
(Inaudible.)

M
Sure. The focus on intermediaries, the importance of intermediaries. Several of you made this point and it strikes me that the maximalist solution here tends to want to envision a kind of perfectly constructed, end-to-end architecture from the federal government all the way on down to the patient, but certainly down to the individual provider, and that strikes me as the hardest way to look at the problem. It strikes me just based on what a number of you have said; that if we can understand something about setting expectations for how everyone interacts with providers we can kind of create almost sort of a safe harbor for everyone to start to get over some of the trust questions.

We have some amount of, and so, Todd, when you say this is not a technology problem I agree with that 100%. I think that the trust and authentication and identity problems that we have here are partly just social; that the communities have to adjust, have to feel comfortable about interacting, but it's also legal, because both the government and the payers and the providers all have to ultimately decide that they're willing to trust so that they don't face legal liability. I think the classic role for government is to establish those sensible expectations about what everyone's liabilities are so that they can proceed and mostly not worry about it.

I guess I think understanding the responsibilities, the obligations on intermediaries, whether they are providers themselves, whether they are vendors who stand in the place of providers strikes me as very important and from that it seems that we could enable a lot of interaction and information exchange once everyone knows that when they're dealing with some unknown point out there, whether it's a payer or another provider or a lab or anyone else, that there is some cover level to kind of a generic point. I guess what I think that implies is that we focus a whole lot less on specific technical – well, that we ought not to try to specify the technical behaviors of these intermediaries, but we ought to think more, and I would suggest we go back to our four scenarios and really think about the expectations we have on the intermediaries in the case of each of those. I think if we could actually clarify those – I think in the end if the ONC could clarify those for everyone who is expected to function in this community people could just start functioning with greater certainty and less worry. I think the way to get to kind of Wes' interoperability begets interoperability is to introduce just a baseline of certainty in a limited set of interactions and from that it will grow and there will also be some questions that will require people to fight a little bit or new rules to be written or whatever else, but we won't know what those are until we get started. Thank you.

M
So we have – there is a Policy Committee meeting next Wednesday and I think we are invited to at least summarize how far we've come in our deliberations and if we are prepared to make recommendations we'll have that opportunity. We have a few days of off-line consultation available to us between now and then. I've heard kind of an emerging framework that we talked about a little bit and Danny just reflected is to go back to the use cases that we had in our first meeting agreed were the shaping tools for our discussion that engaged interoperability in some degree and maybe we should review those use cases with an eye to these risk levels and seeing whether they can be classified either across the board or with some granularity in terms of these risk levels and therefore, the associated authentication and proofing requirements. That would, by itself, be a kind of educational exercise for us and for the Policy Committee. Then I'm wondering if Danny's last suggestion that, in a sense, simply speaking to this will be educational and will stimulate some behavior in the market will be helpful.

M
What Wes pointed out was very thought provoking; that most of the context here was remote access to applications and the potential for risk from them. This has been something that's been bugging me for a long time is the point that was made. If I'm a physician working in an emergency room in that physical location, having logged into the clinical application there, the standards that that organization has, I mean the amount of risk and danger is enormous, right? I can write orders. I can change orders. I can change

clinical information. People’s lives are literally at stake. I am in the system now, right? Yet, we’re saying if you want to send something, a prescription out of that organization we’re going to look at the risk level and say that the authentication done to allow me to access that clinical application in that physical location in the ED is now somehow insufficient and I need to have a token to send that? It doesn’t make sense to me.

W
I would say that that’s because one of the things that does make this environment seemingly a little different than a lot of the things we’ve heard in testimony is this notion ... contextual authentication. That is we saw some of it – we heard about some of it, but the context, I think the example that was given to us is he got in the emergency room. He’s acting as a doctor. People are there. It’s a small room, so that provides its own level of a kind of authentication. So that if we were going to have to go through the exercise of doing a risk assessments those are the kinds of things that would actually come into it and then you end up with what somebody else might call a level one or two being the practice that’s instituted in a much more closed environment or particular context. So there’s a lot of context in healthcare, a lot of it and it will change so that you don’t necessarily have to have the same token to do everything I want to do.

M
Another way potentially to think about it is the two factor is what you know and something, what you have or who you are or where you are potentially. The physical location, I’m on the network and being on the network is my second factor. If I want to remotely do this from home then okay, now that’s a different story. But if I’m physically on the network that will then use the server-to-server then that is my authorization.

W
No, but ... I wouldn’t make it quite that broad. It might be I’m on the network doing a particular task because the task does matter. It’s not just that I’m on that network, I’m on the hospital’s machine.

Another reason I think we have to look at context if you want to do it is just simply, surely it goes back to workflow, which is so intimately linked to legacy systems. Even if you have high compliance in terms of the number, high penetration in terms of the number of people who will ... to buy new systems there are many things in their environments that they’re not going to be able to change. There are these great stories from the Institute of Medicine study that just came out when you talk to some of the people who participated in that study when they went around to the hospitals. One of the stories was there were these three machines and in order for the service to be provided to the patient in this hospital setting the doctor who is prescribing the treatment has to be logged into that machine, but that doctor can’t physically be there because it has a time out and so forth, so there is a nurse whose only job on that floor is to go around and make sure the right doctor is logged into the right computer.

There are a lot of stories like that in their report when you interview them and so the point is that they ... maybe what we’re really talking about is when the data is crossing boundaries, because you can’t do too much inside of that organization because you’re going to hit up against all of these kinds of weird legacy system problems and equipment problems.

M
I guess what I’m getting at, what made me a little nervous was to say let’s go through the use cases and do the risk assessment that the missed tool would have us do and then apply those risk assessments to if you use an EHR for interoperability; if you use it for your clinical care that doesn’t apply; but if you want to send a prescription then now all of the sudden this higher level of authentication applies.

M
Why does that make you nervous?

M
Because it imposes new workflow demands that are not present in this. The activity is just as risky when you do it within the walls, right? But now if you want to send a prescription it imposes new workflow requirements. If we think about the provider-to-pharmacy, provider-to-payer, provider-to-lab, provider-to-provider interactions that are currently taking place with EHRs we're trusting the EHR vendor as the new intermediaries do that.

M
That's right. So let's just take the provider-to-provider care summary transmission just because it's sort of our simplest case, right? I think I might send you through whatever environment we describe here, whatever ends up being the approved way of doing it meets whatever requirements we say it ought to meet, you say it ought to meet. It's certainly possible that once I send it to you there could be an authentication failure in your system; that nurse could actually be an identity thief or any number of things and I would just suggest to you that's not our problem. It is, I think, a HIPAA problem. I think there are all kinds of other laws for which it's a problem, but it is not. I think the part, the sentiment in which I agree with you is we should think about the fact that we're obviously imposing another layer of workflow. We should make sure that that's as manageable as possible, but I think we should resist any security problems that don't directly arise out of these scenarios. We have to assume that the systems are well enough designed to handle those other problems and if they aren't, that there are legal consequences or at least financial consequences or some consequences for failure. Unless, I mean Latanya will tell us, I'm sure, if the thing that we suggest for interoperability would end up creating a new security hull, but the existing ones we shouldn't try to fix. I hate to say it.

W
The thing that I'm not sure – I don't know – anyway, what if is it okay to assume – I'm thinking about the study that we heard at the last Policy Committee meeting that told us that some wildly frightening amount, like 60%, of healthcare providers aren't doing the annual risk assessments that they're supposed to do by law under HIPAA. So I get that that may not be our problem in particular I think is what you're saying, but is it okay if we compound the problem and give rise to a new problem, which is that under Farzad's scenario is it okay just to accept that particular practice at an institution that maybe they haven't done a risk assessment in a decade and really don't care to do one, but now they're introducing new problems onto the network and creating other ones for everybody else. I mean is that an okay assumption to have?

M
... thing is them not doing the risk assessment is a general problem and should be treated as a general problem, not doing something different for interoperability because that problem – we're doing risk assessment as part of meaningful use to address that problem more broadly than just trying to be more secure on interoperability because there might be a problem with risk assessment at a local site.

W
Yes.

M
I just think we have to assume that there are HIPAA mechanisms, there are state regulatory mechanisms, there are whatever other sets of mechanisms, which may not be working well I mean, but the only way that we could possibly address those problems is to say that you actually can't exchange data with

another provider who hasn't certified that they've met all of these other security best practices and legal requirements. Now, there are environments in which that's what happens. I mean that's, to a certain extent, what banks do; that's, to a certain extent, the way that a lot of other financial networks work is that they're not going to talk to you; your system is not going to talk to them unless you've seen their audit statement and all kinds of other stuff. I don't – I think it's a big step to say we want to go there. I'm not saying it's – I think it's a big step and I guess I think we have to believe that –

W

... JACO would provide or NCQA or they just don't do that? It's not a part of their accreditation?

(Inaudible voices.)

W

Oh, so it's maybe not a balanced place to push?

M

I heard some shaking of heads about the idea of reviewing the use cases. Several people didn't like that direction in terms of the risk assessment and the granularity of the context and so on.

M

Latanya said that context is part of the risk assessment. I think part of it is a lack of knowledge about how this risk assessment would take place. It's quite possible that if you did the risk assessment properly that takes into account the context it would turn out that if you're on an EHR system that's in an organization that maybe that is level two, assurance needed and puts you in a different context. But do we know enough about the risk assessment I guess is –

M

(Inaudible.)

W

The risk assessment that Peter talked about from NIH, the one at Carnegie Mellon, that's not something we could just casually do. Those risk assessments that they were referring to are pretty sophisticated. Yes.

M

Thank you. Wes.

W

We could do a back of the envelope thing to see if we felt that there was enough variability there, but I don't think it's something that could be done easily –

M

Yes. I think Danny's point that we are really asking a question about how do we – do we just shut down interoperability. I mean we already have a level of interoperability, which is trivial in terms of the volume of data that can be passed, but nonetheless, what's the trust requirement on the recipient and that's the fax machine. If I fax something to another doctor's office I either understand that that became their liability or I trust them, one or the other; either way, I'm not taking liability for it any more. That's organizational trust and we understand that when we greatly amplify the amount of data that can be spent that way, the consequences of casual organization, promiscuous organizational trust, if you will, get higher. But if we get this far into uncharted territory in terms of where, in terms of the mechanisms for establishing audited trust of organizations where we're sending information then I don't see a way to meet meaningful use requirements in 2012.

M
You're saying that for the installed based for EHRs in the country at that time?

M
Well, you bring up a different question. Do we care about an EHR user inter-operating with someone who doesn't have an EHR, but might be able to get e-mail? Obviously, I think that's important, but whether we want to make that a criterion or not in this discussion I don't know. But fundamentally we operate now in an environment that carries risks about information sharing and we understand that we're going to amplify those risks, but I just wonder what's the best way to go forward. Is it to just stop; don't do anything and then get through an unknown quality of technology at an unknown cost in order to start again or do we try to find some middle ground?

M
Latanya.

Latanya Sweeney – Laboratory for International Data Privacy – Director
... with Wes, because I'm going back to –

M
I just want to follow up on that because I mean I'd be curious what the group thinks about that question. Are we talking about the installed base, the meaningful use of the installed base in 2011 or are we talking about something else? I'm not saying that it has to go you're only talking about EHR-to-EHR, but I'm saying it comes from EHR at least, so are we talking about that? Because it changes a lot of this.

M
So it may or may not. It certainly – I guess I think that I just think of the bottles of the payment systems and what I know, which is relatively little, about the clearinghouses. I mean my understanding is that there are lots of different ways that different providers interact with the existing payment systems. Some of them are able to do it with their own systems. Some of them do it through third parties. It seems to me that our goal would be to be generic enough that any provider could participate.

M
That doesn't work good. The analogy falls short because when you're talking about payers and paying payers 95% of the providers do have a system that they can submit from. We're talking about a situation where maybe 20% to 30% will have a system, so it's a different thing. Now, how you handle it once it comes out of that system is what you're talking about, different ways to do it. But you're talking about a situation where 95% plus already are coming out of the system.

M
I mean look, Danny, when you're talking about the meaningful use use cases the reason we're talking about those is because there is a particular governmental responsibility as part of this incentive program for meaningful use of certified EHR technology.

Danny
That's for the originators. I'm thinking, for example, in the case of the referral.

M
Yes. Yes, but again, you're now talking about 20% of the providers in the country versus 95% to 98% in your example.

M
But that's going to grow.

M
I'm sure it's going to grow.

M
I think we need to put some bounds around this and the bound is interoperable EHRs.

M
Okay, because I think that may change some of these discussions.

M
There could be people who would like to speak. We are coming to the end of our public session time. There may be people on the phone who want to speak as well. Then we're going to adjourn this meeting in a few minutes and there may be other conversations that happen later.

Let's see, people who want to make comments that are ... to today's authentication meeting and to this set of issues that are now on the table, let's get those wrapped up so we can finish and then come back to the broader questions, the findings of the committee and so on, later. For those of you who have your signs up, Latanya, Carol, Arien –

Latanya Sweeney – Laboratory for International Data Privacy – Director
I'll tell you what I was going to say: I don't think we should necessarily discuss it in this time, but I was going to just clarify back to your earlier point about the risk assessment. When they were talking about risk assessment they meant a rigorous thing, but for us to move forward we probably have to do some kind of back of the envelope kind of risk assessment because even if we don't do it we sort of do it implicitly anyway and so it would be better if it were done more explicitly.

M
Yes. I agree with that. Carol.

M
I think we're going to say very similar things, but with regards to doing risk assessments, one of the things that we heard over and over again is that we need to push this problem as close as possible to the provider and that ultimately everything relies on a policy and contractual framework that governs that interaction. At the end of the day what we're caring about in the use cases that we're talking about is I'm provider B. I receive information from provider A. I just need to know that provider A, that this truly does come from provider A and provider A is electronically who provider A purports to be. At the end of the day we can't – I don't believe we can over policy this except by pushing this down to the organization that's authenticating the provider, making sure there's some legal ... to the policies that that organization implements and making sure there is legal ... to the contractual relationship the provider has with that organization and that if those three things are in place you've got a certificate that you can sign on that transaction, you can sign that transaction such that provider A knows that it came from provider B and vice-versa. I'd like to side-step a lot of this risk assessment discussion to what I think is the more

germane discussion about what's the right policy framework for an organization contractually to apply in authenticating the providers.

W
I think I'm struggling with the question we're trying to answer a little bit, but going back to the premise that provider A wants to send provider B the summary it seems to me there are three things we need to consider. One is is provider B who they say they are. If there is a role for government in helping to automate that function because the government's maintaining the national provider identifier and paying hundreds of millions of dollars of claims against that database then we should consider it. In other words, it's a way to validate it's a real provider. For those of you familiar with what we did in Katrina Health, we essentially used the AMA master physician index in a similar way, which was that they had a lot of information where they could do knowledge base authentication of providers and that worked. So I need to know who they are. That's one set of problems.

I need to know they have a valid certificate from a valid issuer that I can trust.

The third piece; and I think this is the biggest challenge and this is why the consumer space and the provider space are different; is I need to police it. I need to have mechanisms for oversight and redress. The regulatory and legal framework, if I'm a physician and licensed and subject to fraud and abuse laws and all kinds of other things it is very different than what an individual might be subject to when they're on the Web. I do think that that makes a big difference.

One of the reasons I was pressing today in the questions about oversight is that to some extent the more transparency about these trusted authorities, whoever they may be, exist in the system the more pressure there is for them to live up to whatever initial bar they were tested to meet. I think that's certainly an area of consideration, but I'm worried that we're making this – we're bleeding into other areas beyond the I want to send a document to someone and I want to know that I'm sending it to the right person.

M
Do you have a last word, Wes, before we adjourn?

Wes Rishel – Gartner, Inc. – Vice President & Distinguished Analyst
Yes. I just want to, because Dan mentioned clearinghouses, I just want to perhaps redundantly repeat myself. There is a difference between sending transactions over a network and giving remote access to an application. Virtually everything we are talking about in terms of stage one interoperability criteria involves sending something over information, even e-prescribing. Typically I enter an order into this system and that systems sends an order for that. There we have an obligation to make sure it's auditable. We don't have an obligation to pass the trust on to the other system and I think it's important we keep that in mind.

M
Before we adjourn can I just check the temperature of the group in terms of how many folks think that intermediaries need to be a part of the authentication story?

M
Everybody almost, except for Jim.

M
So one alternative would be centralized credentialing of every provider that does not rely on the –

M
Yes ....

(Inaudible voices.)

M
Are you talking about like an independent third party that would be a part of the authentication or identity proofing process? For instance, and this is really what I'm getting at, I think we know that as a part of the hiring process most hospitals will go through an I-9 process. They will do a certain level of required identity proofing, if you will, as well as employment eligibility checks.

M
What I'm referring to is what I think we've been talking about of do we try to do authentication to the provider and that provider holds something; we're talking about for level three; the provider holds something; the provider has to have a token. The provider has to have the PKI. The provider has to have something. Or do we think that for the four meaningful use use cases we're talking about here we think the certificate holder can be the information service provider and the authentication is delegated to that information service provider without having necessarily the end user be requiring that the end user hold a hard token?

Latanya Sweeney – Laboratory for International Data Privacy – Director
That question has so much stuff embedded in it.

M
I know. I know.

Latanya Sweeney – Laboratory for International Data Privacy – Director
In every one of those there are lots of options, but you just took one path through lots of options.

M
I agree with you, Latanya. Let's look at this the same way we've looked at meaningful use itself, which is that it is a three-tiered progression along a trajectory that may start at a relatively modest level and that will step up to a higher standard as time goes on. Of course, that carries with it the very real risk that given the way the incentives are structured there will be providers that will never get past the first level. But I mean, certainly, moving from a less robust authentication and perhaps identity proofing strategy to a more robust strategy over time and framing our recommendations within that context would, I think, be appropriate.

M
Well, I think it sounds like it's premature or complex to answer your question in a tidy way. I think given our timing and where we are at this moment it would be helpful if the staff collectively could synthesize today's testimony and not so much report it back, but try to collapse it into some categories and questions that have emerged from our discussion so that we can then collectively take a look at those and say, much as Jim just did and Latanya, what are the layers that are embedded within each of these pathways that we've talked about. I think we're going to need another dive analytically into the complexity of the problem, but right now we don't really have a tool to even do that except more conversation, which I think we're out of time for. My request would be if the staff can, in a few days, turn something back to us that helps with that; that would be great.

Farzad, any other suggestions?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
It would be good if we had some simple, high level recommendations pertaining to authentication for next week. It would be good. It may not be possible, but it would be good if we could get –

W
How about authentication as needed?

M
It's good. I like that. I don't know; there may be such high level findings in the summary that ... presented at least fairly obvious. I think it's also good for us to remember that the Policy Committee as a whole and other audiences haven't had the benefit of this much exposure to the issue and we can probably say some things that to us now seem fairly clear that weren't clear three months ago and maybe that will be helpful by itself.

Any more comments?

Farzad Mostashari – NYC DH&MHH – Assistant Commissioner
No.

M
So without any further discussion then we are adjourned for this meeting. Thank you, all, and thank you to our guests for joining us today. We're adjourned.

Public Comments

1. College of American Pathologists: Has the panel look into the policy that is established within DOD and the VA for Transmission and Health care records security? I am sure SecDef Gates would be glad to share, and not recreate the wheel.

2. Basic Issue is this. Directories discussed and services today are based on an administrative, transaction, payment, authorization focus. However to date they have not focused on the demographics necessary for patient directed consent, public health needs, quality reporting & analysis as well as patients directions and or contact info for referrals. I would hope that there is a focus on the later which does not exist today in most cases as both SSa and CMS indicated.
Steve Witter, Vice President Folio Associates. 508.280.9000

3. In regards to data back-up and meaningful use: I would like to hear more about how once all of this data is placed into all the new EMR implementations in private practice and hospitals that it will be protected from loss. Currently HIPAA requires covered entities to back-up data but most do not do this and those that do, do so in-house, ergo if the office is lost due to disaster so is the backed up data. Others use cold storage for tape and optical disk, but this does not comply with the intended use and spirit of the NHIN; specifically exchanging data over the Internet, and Time-sensitive access to medical data during a disaster.

4. DEA has the ability to fine a clinician if they do not report an address change within 30 days as well. Has anyone ever been fined for not updating their DEA ADDRESS?

5. Has there ever been a fine issued by a state board for a physician that did not change their address?

6. So if a physician maintains a NY license but has moved to Florida where they practice. How do you know which address/states the physician actually practices at?

7. How many of state medical boards then verify address information?

8. Do you maintain more than one address for a physician, for their group practice relationship?

9. Do you maintain a cross-reference of license information to NPI?

10. How often is the address, phone, fax information updated? Are these elements only taken from the license file or are they verified with the provider?

11. As Jim Borland said there are very different pieces of maintaining a provider directory. Payment, authorization data is very different form the provider demographic data necessary for patient directed consent, quality reporting, public health needs and forever providing patient’s directions and contact for referrals. To date the provider directories are focused almost solely on transaction, payment and authorization only.

12. Two parts to Accuracy - The is a different level of detail.security and information necessary for a healthcare payment to be made. The data demographics required for referrals, giving patient directions, Public health reporting, quality reporting and administering patient consent is much different than the authentication/payment transaction.

13. More oversight is clearly required. Today it appears a closed and not transparent set of activities and use of incentives.

14. Additional the directory services errors are the number one issue when you look at the information provided at the surescrpts workshops to all there participant vendors and partners.

15. Do you supply provider data into the provider dictionary in a providers EMR system

16. This an excellent example of another potential service that is being inhibited to provide a completive alternative to surescrpts. The current market owners of surescrpts are a very limiting factor. again the cost being proposed for med reconciliation is not consistent amongst its members and is also leading to a potential diversion of array funds to cover this cost with the state based HIE's . This has become a visible issue with the current rfps being considered at the state level for e prescribing. This is unfair competitive practice and is a potential violation of the current by laws with the ss contracts. Examples would be Maryland which is in the process of awarding a contract as well as other states. The intent of the funds was not to pay the pharmacies and mail orders for the access to med history which is a critical data source to drive compliance.

17. How does your data allow you to administer patient consent to the individual provider ant a specific location?

18. What is the accuracy of the provider directory... first related to the unique provider identified? Secondly what is the accuracy of the demographics (address,phone,fax,practice,relationsips). How often does the primary address phone or fax change in your experience

19. If credentialing period is two years, does someone have to update the data in the interim

20. How often are they required to verify the data?

21. Tighter oversight is required with the amount of government incentive being driven there way

22. This could be significantly improved and they have created an approach. They have to dare not shared this improved efficiency as a fear of a competition.

23. Thank you for recognizing the differences in how the directories are formatted across the spectrum of provider types. Question: the elements that were described to be included in the directory, how were these determined and are there still options to review and recommend any additional elements. Thank you.

24. 2 questions how surescrpts is addressing the significant potential and occurrence of errors in the directory download process. This is a very time consuming and inhibitor of proper workflow. Second question, how is a private entity operating a public service with very little oversight and with the potential to inhibit the intended success with potential inconsistent pricing of additional services like med history

25. Laura McNulty, ESRI: is there a presentation to support Ms. Mahan's testimony?

26. Pam Mason: Will the public be able to get copies of the slides?